

(別添1)

電子署名及び認証業務に関する法律の
施行状況に係る検討会報告書

平成20年3月

目 次

はじめに.....	1
第1章 電子署名法の施行状況	2
1. 電子署名法の目的	2
2. 電子署名法の概要	4
3. 電子署名法の施行状況	7
第2章 検討結果	13
1. 電子署名に用いる暗号技術の安全性向上に係る方策について（技術的論点）	13
2. 認定認証業務における利用者の真偽の確認について（制度的論点）	22
3. 普及促進策について（ビジネス的論点）	25
4. その他の諸課題.....	27

凡例：

「電子署名法」又は「法」

… 電子署名及び認証業務に関する法律（平成12年法律第102号）

「電子署名法施行規則」又は「施行規則」

… 電子署名及び認証業務に関する法律施行規則（平成13年総務省・法務省・経済産業省令第2号）

「告示」

… 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成13年総務省・法務省・経済産業省告示第2号）

はじめに

「電子署名及び認証業務に関する法律」（平成 12 年法律第 102 号。以下「電子署名法」という。）は、平成 12 年第 147 回国会の審議を経て、同年 5 月に公布、平成 13 年 4 月 1 日に施行された。

電子署名法附則第 3 条において、「政府は、この法律の施行後 5 年を経過した場合において、この法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずるものとする」とされており、総務省、法務省及び経済産業省（以下「主務省」という。）は、平成 18 年度以降、外部有識者のヒアリングを行うなどして同法施行上の課題の抽出等を実施してきた。

電子署名及び認証業務に関する法律の施行状況に係る検討会は、これまでに抽出した課題について議論を行い、今後の電子署名法の運用に反映していくことを目的として、平成 19 年 12 月 18 日から平成 20 年 3 月 31 日までの間に計 3 回開催された。本検討会では、電子署名法の施行状況を調査し、関係団体からの意見、要望を受けて、検討課題の整理・分析を行い、現行の電子署名法における課題を大きく技術的論点、制度的論点、ビジネス的論点に分けて議論し、検討を行った。

以下に、平成 19 年度、本検討会において検討した結果を報告する。なお、政府は主務省を中心にこれを受けて必要な措置を講じるとともに、更なる検討が必要な課題については適切な検討体制の下で継続的に検討を行っていくことが望ましい。

第1章 電子署名法の施行状況

1. 電子署名法の目的

(1) 電子署名法制定の背景

近年、インターネットを始めとするネットワークが、従来の企業間通信のみならず、国民生活一般にまで浸透してきており、我が国の社会経済活動にとって必要不可欠の存在となってきた。

このような状況の中、インターネット等においては、相手方と対面せず、電子的なデータである情報をやりとりすることから、情報の受信者が、発信者が本当に本人であるのか（「なりすまし」の可能性）、情報が途中で改変されていないかどうか（「改ざん」の可能性）、発信者が発信していないと否認するおそれはないか（「送信否認」の可能性）等の脅威に対応する必要性が生じてきた。

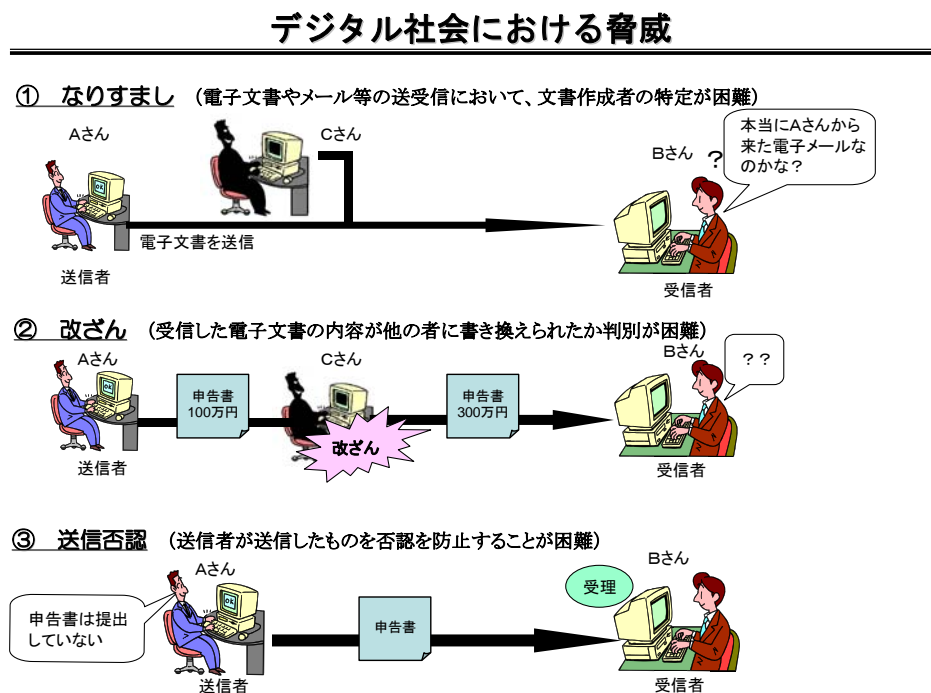


図 1-1

上記のような脅威に対応する手段として、暗号技術を応用した電子署名及び認証業務が利用され始めてきた一方、平成12年以前においては、電子署名や認証業務が本人確認等の手段として利用されたとしても、我が国ではそれが法的にどのように取り扱われるのかが定まっていなかった。すなわち、後日、ネットワークを通じた情報の授受について当事者間で争いが生じた場合に裁判所でどのように評価され、解決されるのかが、手書きの署名や押印のような明文の規定がなく、電子商取引等の普及の妨げになっているのではないかという指摘があった。このような背景があって、電子署名法が制定された。

電子署名の基盤となるPKIの仕組み

PKI (Public Key Infrastructure: 公開鍵認証基盤)

- PKIとは、公開鍵暗号方式に基づく電子認証の技術基盤
- 具体的には、秘密鍵による暗号化(電子署名)、公開鍵による復号化、公開鍵の電子証明書を組み合わせ
- 本人性の確認や文書の改ざんの有無の検知を行うもの
- 公開鍵の電子証明書を発行し、その有効性を証明する第三者機関が認証局(CA: Certification Authority)

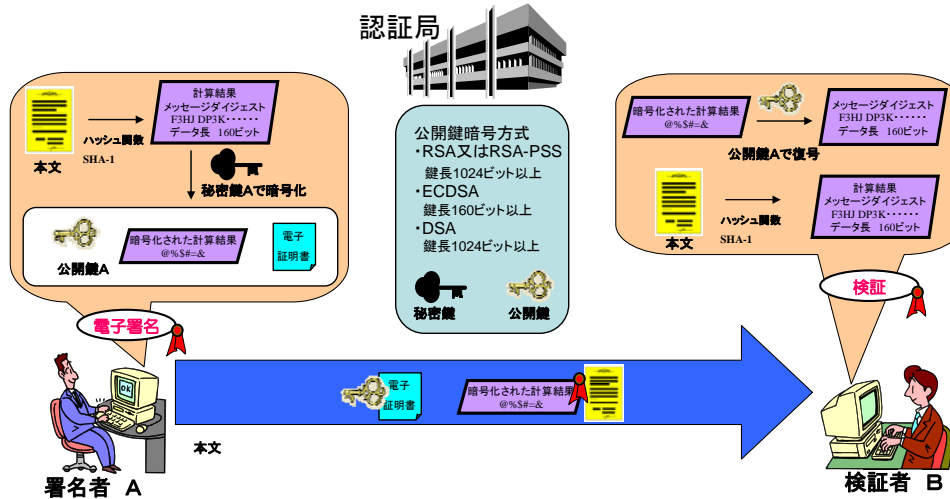


図 1 - 2

(2) 電子署名法の目的

電子署名法においては、電子署名に関し、電磁的記録の真正な成立の推定（法第3条）、特定認証業務に関する認定の制度（法第4条等）、その他必要な事項を定めることにより、国民による電子署名の円滑な利用を確保し、電子商取引を始めとするネットワークを利用した社会経済活動の一層の推進を図ることとしたものである。

電子署名法の目的は、法第1条に以下のように規定されている。

第1条 この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする。

2. 電子署名法の概要

(1) 電子署名及び認証業務の定義と要件

第2条 「電子署名」とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

- 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
- 二 当該情報について改変が行われていないかどうかを確認することができるものであること。

電子署名法第2条第1項の「電子署名」の定義は、この法律が適用される電子署名、認証業務等の範囲を限定するものである。そこで、いわゆる技術的中立性の要請に配慮し、電子署名の方式、方法等に着眼した定義を避け、電子署名の機能等に着眼した定義を採っている。同項第1号はいわゆる「なりすまし」防止に対応するもの、同項第2号は「改ざん」防止に対応するものであり、これら2つの脅威への対応がなされることで、もう一つの脅威である「送信否認」も防止することができる。

また、電子署名法の体系では、認証業務を3段階に定義している。電子署名が行われた情報を受け取った者は、電子署名を行った者が誰であるのかを確認する必要があるが、認証業務とは、その確認のために用いる情報が利用者に係るものであることを証明する業務のことである(法第2条第2項)。また、この中から主務省令で規定された基準に適合する電子署名について行われる認証業務を「特定認証業務」(法第2条第3項)、さらに、設備や業務の実施方法に係る基準を満たし、認定を受けた認証業務を「認定認証業務」(施行規則第6条第2号)と称している。

電子署名及び認証業務について

電子署名 (法第2条第1項)

「電子署名」とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

- 一 当該情報が**当該措置を行った者**の作成に係るものであることを示すためのものであること。
- 二 当該情報について**改変が行われていないかどうかを確認**することができるものであること。

(法第2条第2項 認証業務)

「認証業務」とは、自らが行う電子署名についてその業務を利用する者(以下「利用者」という。)その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

認証業務

技術的基準をクリア

(法第2条第3項 特定認証業務)

電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

特定認証業務

主務省令で定める基準(施行規則第2条、指針第3条)

- ・RSA方式(SHA-1)1024bit以上
- ・RSA-PSS方式(SHA-1)1024bit以上
- ・ECDSA方式(SHA-1)160bit以上
- ・DSA方式(SHA-1)1024bit以上

設備・業務方法の基準をクリア

(法第4条第1項 認定)

特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

認定認証業務

(認定の基準 法第6条第1項)

- ①業務の用に供する設備の基準
- ②利用者の真偽確認の方法
- ③その他の業務の方法(業務規程の策定、利用者への説明等)

(法第4条第1項の認定を受けた認証業務)

図 1 - 3

(2) 電子署名法の枠組み

電子署名法の内容には、大きく分けて2つの柱となる規定が存在する。

一つは、電磁的記録に本人による一定の電子署名が行われている場合に、成立の真正を推定する規定（民事訴訟法第228条第4項に相当するもの）である（法第3条）。もう一つは、特定認証業務を行おうとする者は主務大臣の認定を受けられることができるという規定（法第4条）であり、認定認証業務の電子署名に関して上記の推定規定が司法の場で適用されやすくなることを期待しつつ、国民に対して認証業務の信頼性の目安を設けようとする制度である。

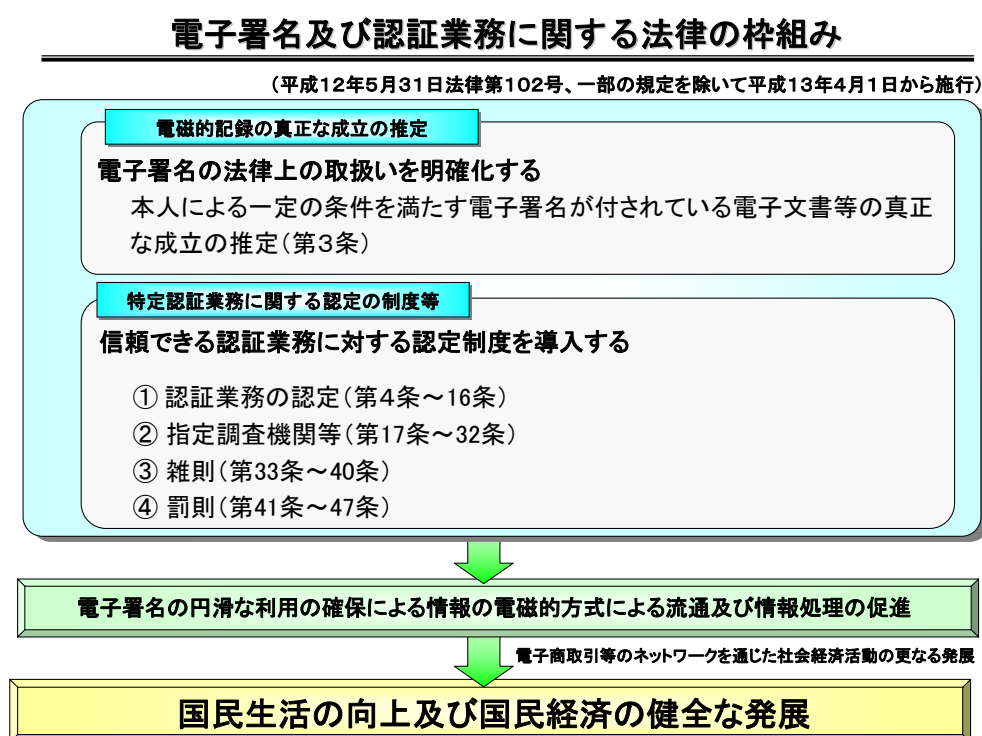


図 1 - 4

(a) 電磁的記録の真正な成立の推定

民事訴訟法第231条により準用される同法第228条第1項によれば、準文書（情報を表すために作成された物件で文書でないもの）を証拠として用いるには、その成立の真正（当該準文書の内容が、挙証者の主張する特定人の意思に基づいて作成されたものであること）を証明しなければならない。そこで、電子署名が行われた電磁的記録を準文書として提出する場合にも、証拠調べを請求する者は、その成立の真正を証明しなければならないところである。

民事訴訟法第228条第4項は私文書について本人の署名・押印があるときに当該私文書の成立の真正を推定するものとしているところ、電子署名法第3条は、これと同じ趣旨の規定として、電磁的記録に記録された情報について一定の要件を満たす電子署名がされているときに当該電磁的記録の成立の真正を推定するものである。

電磁的記録の真正な成立の推定

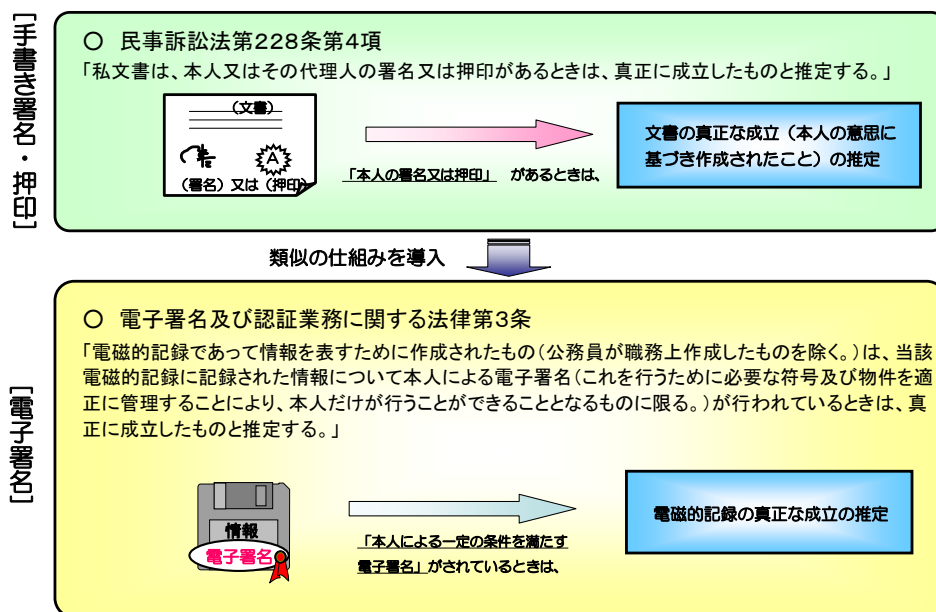


図 1 - 5

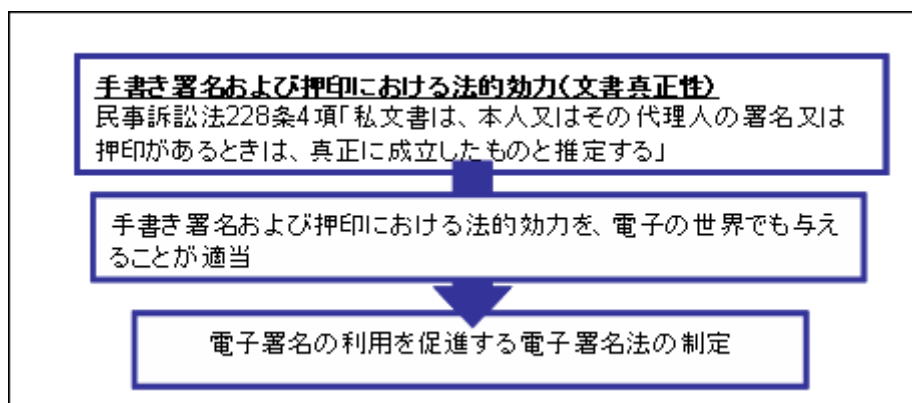


図 1 - 6 電子署名法制定時の考え方

(b) 特定認証業務に対する任意の認定制度

特定認証業務は、国民がネットワークを利用して情報のやり取りを行うに当たり、安心して電子署名を利用することができるよう、一定の技術的信頼性を有する電子署名に係る証明業務であるが、その前提として当該業務が信頼できるかどうか国民にとって重要となることから、認証業務の信頼性の目安となるよう、電子署名法第4条第1項において、主務大臣が認定を行うことができるとされている。

市場の自由な発展を阻害しないため、認定は任意的なものとなっており、認定を受けなくても特定認証業務を行うことは可能である。また、認定の法的効果として、当該業務が認定を受けている旨の表示が可能となる（法第13条第1項）。

認定の要件としては、以下が規定されている。

○申請者が欠格条項に該当しない者であること（法第5条）

禁錮以上の刑や本法違反による刑に処せられた者又は認定を取り消された者等は、一定の期間認定を受けることができない。

○申請の内容が次の基準に適合するものであること（法第6条第1項）

①業務の用に供する設備の基準（第1号）……電子証明書の発行に利用する「発行者署名符号」の厳重な保管、安全・信頼性を有する設備の使用等

②利用者の真偽の確認の方法（第2号）……公的機関の発行する身分証明書等の提示を求める等

③その他の業務の方法（第3号）……認証業務の実施に関する規程を定め適当な権限分散を図っていること、失効リストの適切な開示等

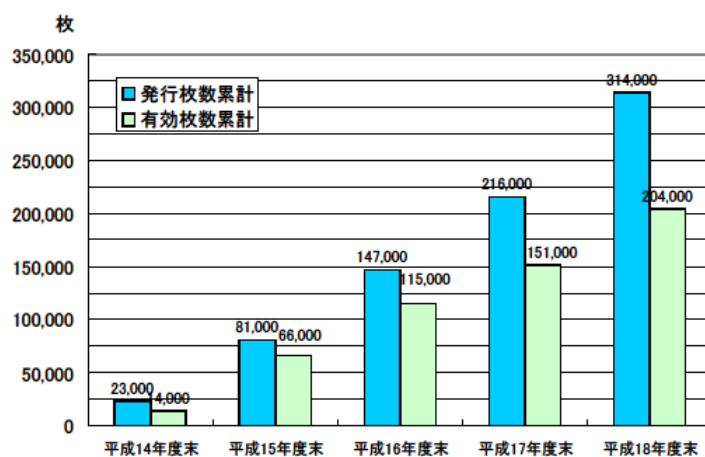
このほか、認定認証事業者には、認証業務に関する帳簿書類の作成・保存義務（法第11条）等が課せられている。

3. 電子署名法の施行状況

（1）認定認証業務に係る電子証明書の発行枚数の推移

認定認証業務に係る電子証明書は年々増加しており、平成18年度末現在、累積発行枚数約31万枚（有効枚数約20万枚）の電子証明書が発行されている。

認定認証業務に係る電子証明書の発行枚数の推移



注1: 廃止された認定認証業務に係る電子証明書の発行枚数を含む。
注2: 数字は概数である。



認定認証業務に係る電子証明書は年々、増加傾向

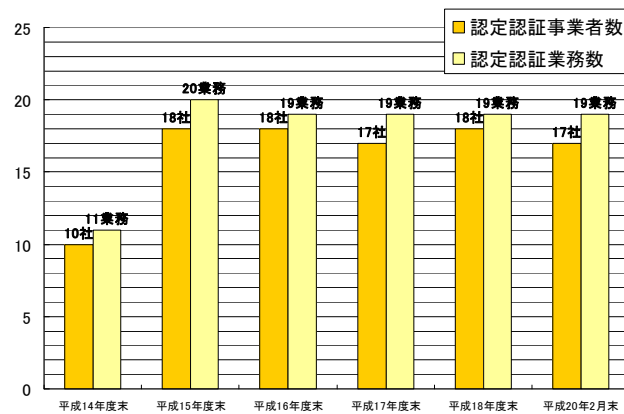
図 1 - 7

(2) 認定認証業務数・認定認証事業者数の推移

平成14年度末には認定認証事業者数は10社であったが、翌年の平成15年には18社と約倍となり、それ以降はほぼ安定している状況である。

電子署名法施行以前には、認証事業者はおよそ4社程度であったが、現在は、認定認証事業者ではない認証事業者を含めておよそ30社程度存在しており、法施行前後で認証事業全体が活性化していることがわかる。

認定認証業務数・認定認証事業者数の推移



(参考)

○認証事業者数

- ・法施行前(平成13年):4社程度(ペリサイン、サイバートラスト、日本認証サービス、セコム)
- ・施行後(平成18年):認定認証事業者17社を含む30社前後に増加

図 1 - 8

(3) 認定認証業務について

認定認証業務の一覧は以下のとおりである。認定認証業務が発行する電子証明書の用途は、電子申請、電子入札、電子契約が主となっている。

電子署名及び認証業務に関する法律に基づく認定認証業務一覧

(平成20年3月31日現在)

特定認証業務の名称	業務を行う者の名称	認定日
Accredited Sign パブリックサービス2	日本認証サービス株式会社	平成13年10月19日
株式会社日本電子公証機構認証サービスIPROVE	株式会社日本電子公証機構	平成13年12月14日
CECSIGN認証サービス	株式会社コンストラクション・イーシー・ドットコム	平成14年 3月26日
セコムパスポート for G-ID	セコムトラストシステムズ株式会社	平成14年 7月 4日
AOSignサービス	日本電子認証株式会社	平成14年 8月29日
e-Probatio PS サービス	株式会社NTTアプライエ	平成14年11月20日
TOINX電子入札対応認証サービス	東北インフォメーション・システムズ株式会社	平成14年12月10日
TDB電子認証サービスTypeA	株式会社帝国データバンク	平成15年 2月 5日
ビジネス認証サービスタイプ1	日本商工会議所	平成15年 3月12日
電子入札コアシステム用電子認証サービス	ジャパンネット株式会社	平成15年 4月21日
全国社会保険労務士会連合会認証サービス	全国社会保険労務士会連合会	平成15年 6月10日
CTI電子入札・申請届出対応 電子認証サービス	株式会社中電シーティーアイ	平成15年 9月29日
よんでん電子入札対応認証サービス	四国電力株式会社	平成15年10月 2日
税理士証明書発行サービス	日本税理士会連合会	平成16年 1月16日
e-Probatio PS2 サービス	株式会社NTTアプライエ	平成17年11月 9日
日本土地家屋調査士会連合会認証サービス	日本土地家屋調査士会連合会	平成17年12月 9日
MJS電子証明書サービス	株式会社ミロク情報サービス	平成18年 3月31日
司法書士認証サービス	日本司法書士会連合会	平成19年 9月21日

図 1 - 9

(民間認証業務のサービスの一例)

認定を受けていない一般認証業務の事例には、フィッシング詐欺対策としてのメール用電子署名に係る電子証明書の発行サービス等が存在する。

(4) 利活用事例

電子証明書の利活用の事例には、以下のようなものがある。

● 電子入札

電子署名・認証業務の利活用事例（1）

電子入札

（コアシステムWebページから）

- 平成15年度以降、国、地方自治体を中心に入札制度の電子化が進められ、紙による入札を原則無くしたことから、稼働率の高い電子入札システムが普及。

平成20年1月	中央省庁	公社・機構等	都道府県	政令指定都市	市町村等
(運用中)	9	6	40	15	166
(開発中)	—	2	3	2	271

【電子入札コアシステムの導入費用例(市町村の場合)】

- ・一括買取方式 5,250,000円 又は リース方式 123,375円／月
- ・保守料 787,500円／年

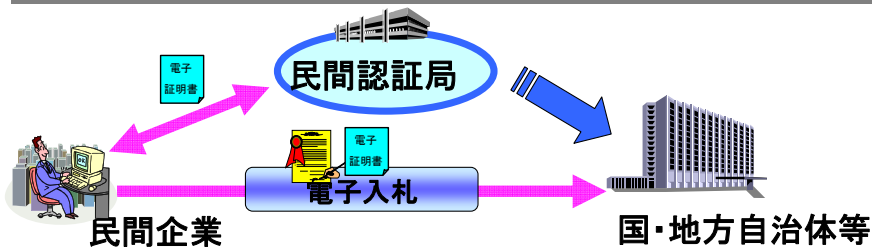


図 1 - 1 0

● 電子申請

電子署名・認証業務の利活用事例（2）

電子申請

- ・国への申請・届出等手続14,149件のうち95%の13,448件がオンライン化されている（平成18年度末調査）
- ・平成19年3月に策定された「オンライン利用促進のための行動計画」の対象手続165件のうち、電子署名の利用を求める手続は134件。
- ・e-Gov電子申請システムへの窓口の移行
各府省が整備した汎用的受付等システムの窓口機能は、e-Gov電子申請システムの一元的な窓口機能に移行する。e-Gov電子申請システムの利用者（申請者）は、移行前は府省毎に異なるシステム環境を用意しなければならなかったが、移行後は一元的なシステム環境での利用が可能となる。

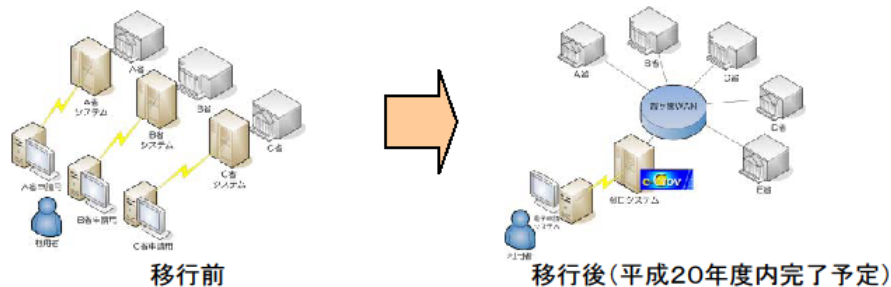


図 1 - 1 1

● 電子契約

電子署名・認証業務の利活用事例（3）

電子契約

- 企業間の電子契約の締結に係る電子署名の利用は年々拡大。
- ◇業務の効率化（契約書の受け渡し時間の短縮、保管スペースの削減等）
 - ◇契約手続の進捗や契約書の案件情報を一括管理
 - ◇過去の契約書を簡単に検索・閲覧

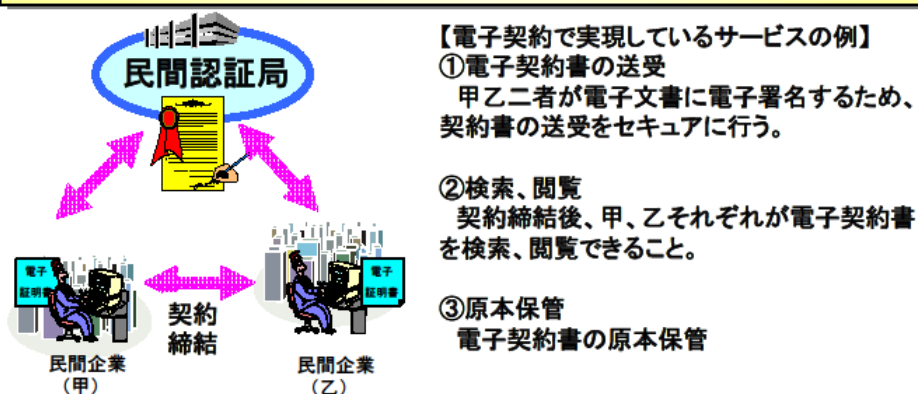


図 1-12

(5) 外国の事例

電子署名法の施行状況の検討の参考とするために、電子証明書の発行枚数が多い韓国の事例を調査した（詳細は、参考資料4を参照）。その結果、韓国における電子証明書の発行枚数は、2006年10月現在で1380万枚であった。その要因を推測すると、以下のものが挙げられる。

- ・電子証明書を利用したサービスが多様であり、一部のサービスで義務化されているなど、電子証明書の利用場面が多い。
- ・（一定の手続で）オンライン発行・更新が可能であり、格納媒体が多様であるなど、電子証明書の取得・利用に係る負担が少なく、利便性が高い。
- ・その他、開始時期が早く、統計対象となる電子証明書の発行機関の対象範囲が広い。
- ・電子署名用途だけでなく、認証用途の電子証明書として発行されている。
- ・インセンティブの付与

(6) まとめ

認定認証業務の発行する電子証明書は、電子入札等のアプリケーションの普及とともに、着実にその発行枚数を伸ばしており、特定認証業務の認定制度は、情報流通・情報処理の促進、ネットワークを通じた社会経済活動の発展において一定の役割を果たして

きている。また、認定を受けていない民間認証業務においても、多様なサービスが展開されるようになってきている。

しかしながら、外国の事例と比較すると、日本に比べて人口に対する普及度が大きい国があるため、その要因を比較分析する等して、我が国の施策の参考にすることが必要である。

第2章 検討結果

1. 電子署名に用いる暗号技術の安全性向上に係る方策について（技術的論点）

（1）論点

電子署名の仕組みの基礎となる暗号技術は、コンピュータの能力の向上などにより安全性が低下する宿命にあり、世代交代は避けられない。現在電子署名法施行規則及び告示で規定されている暗号¹のうち、ハッシュ関数SHA-1及び公開鍵暗号RSA1024bitについては安全性の低下が指摘されている²が、どのような対応を採るべきか。

（2）検討すべき事項

SHA-1、RSA1024bitを用いた新規電子署名の中止を見据え、

- ・ 指針第3条で規定する特定認証業務に係る電子署名の基準に、どのような電子署名の方式を追加すべきか。
- ・ 指針第3条で規定する特定認証業務に係る電子署名の基準からSHA-1、RSA1024bitを用いた電子署名の方式を削除することを含め、どのような措置をどのようなスケジュールで行うべきか。

（3）背景

・ハッシュ関数の安全性に係る状況

ハッシュ関数は、非可逆（一方向）な特徴や衝突発見困難性³を利用して、悪意を持った者による情報の改ざんや機器等の障害によるエラーを検出するために利用できる技術であり、電子署名においても利用されている。

電子文書への電子署名においては、複数レベルの脅威が想定される。

- ・ 電子署名が無い複数の異なる文書に同一の電子署名が付される脅威（衝突計算攻撃）
- ・ 電子署名が付された電子文書と同一の電子署名が別の電子文書に付される脅威（第二原像計算攻撃⁴）

電子署名法は、電子文書に付す電子署名に紙文書における署名と同等の推定効を与える法律であるので、電子署名者による否認を防止できること及び電子署名の信頼性を技術的に確保する必要がある。このためには、第二原像計算攻撃による脅威のみならず、衝突計算攻撃による脅威も含めて想定する必要がある。

近年、従来より少ない計算量で衝突計算攻撃を行う手法が明らかになり（図2-1参照）、要する時間も短縮されつつある（図2-2参照）。

¹ 認定の対象となる特定認証業務において用いることができる暗号として規定

² 暗号技術検討会（総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長の私的研究会として毎年度開催（座長：今井秀樹中央大学教授））等による指摘

³ 同じダイジェスト値を生成する異なるデータの発見に対する困難性

⁴ 別原像探索攻撃とも呼ぶ。英文では、Second Pre-image Attack

ハッシュ関数の安全性に係る状況 (SHA-1)

非可逆(一方方向)な特徴を利用して、悪意や故障による情報の改ざんを検出するために利用

(1) 従来より少ない計算量で同じダイジェスト値を作り出す手法が明らかになった(衝突)



(2) 故意に起こす衝突によっておきる事態

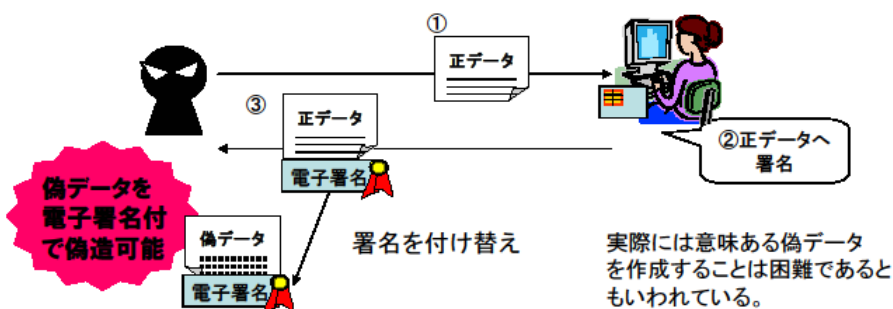


図 2 - 1

ハッシュ関数の安全性に係る状況 (SHA-1)

衝突発見に要する時間の目安 (推定)

SHA-1の実行回数	2006年4月現在
2 ⁸⁰ 回(総当たり)	・国内最高速のスパコンで約100万年
新たな計算 ↓ 方法の発表	↓
2 ⁶⁹ 回	・国内最高速のスパコンで約462年以下

処理時間については、計算アルゴリズムや計算機のアーキテクチャなどに依存して大きく変わり得るため、この年数はあくまで推定である。なお、今後の進歩によっては、スーパーコンピュータだけではなく、インターネットを利用して世界中の国々で分散処理を行う分散コンピューティングシステムによっても、本推定以上の衝突発見能力を実現できる可能性がある。

CRYPTREC 暗号技術監視委員会資料(平成18年6月)を一部補足して引用

図 2 - 2

・ SHA-1 における衝突計算攻撃に要する時間の推定

暗号技術検討会により示された情報によると、SHA-1 の衝突を総当たりで見つけるには 2⁸⁰ 回程度 SHA-1 の実行を必要とし、国内最高速のスーパーコンピュータを用いて 100 万年程度の時間がかかると推定される。一方、同検討会において、新たな攻撃手法 (Wang

らの手法CRYPTO2005) を用いた場合、 2^{69} 回程度のSHA-1 の実行で衝突が発見され、国内最高速のスーパーコンピュータを用いれば462年以下でそれが可能になると推定されている⁵。ただし、処理時間については、計算アルゴリズムや計算機のアーキテクチャなどに依存して大きく変わり得る。

SHA-1 等のハッシュ関数については新たな攻撃手法に関する研究の進展によって、衝突発見までの時間が格段に短縮されるおそれがある。また、今後の技術の進歩によっては、スーパーコンピュータだけではなく、インターネットを利用して世界中の国々で分散処理を行う分散コンピューティングシステムによっても、本推定以上の衝突発見能力が実現される可能性もある⁶。

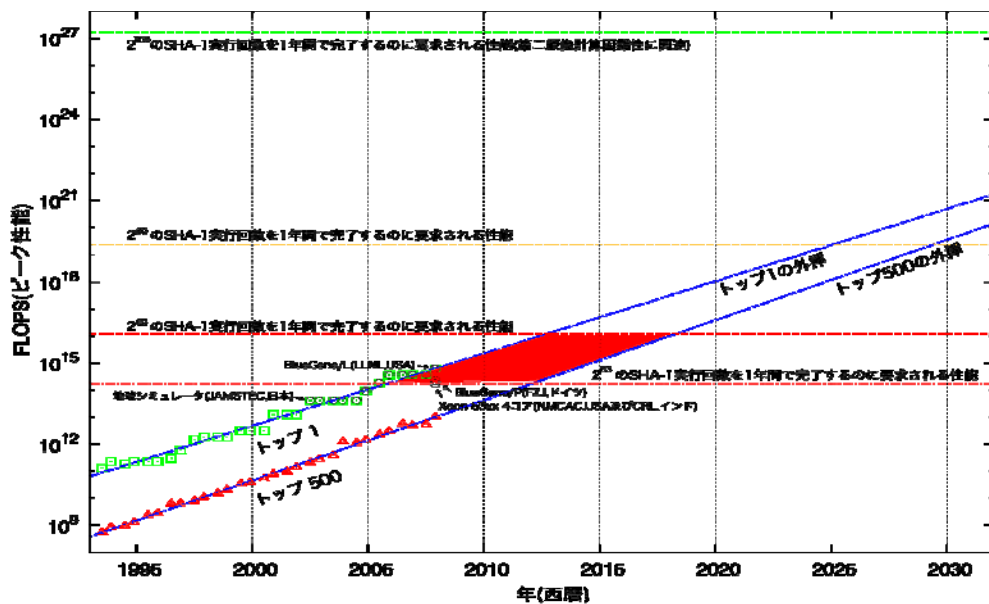


図 2-3 計算機性能の向上及び SHA-1 に対する攻撃に関する計算量の予測

・鍵強度の低下に関する影響

RSA 暗号は、素因数分解問題の困難さをその安全性の根拠としている。長く用いられてきた既知の解法以外に画期的な解法が発見される可能性は低いと言われているものの、コンピュータの計算速度の向上によって、本来秘密にしておかなければならない秘密鍵を公開鍵から導出することが可能となる。

電子署名では、秘密鍵が解読されることにより、電子署名の偽造が可能な状態となる。

⁵ 「暗号技術検討会 2006 年度報告書」(2007 年 3 月、暗号技術検討会) 8 頁「SHA-1 の安全性に関する見解」。

⁶ グラーツ大学 (オーストリア) の研究チームによる実証実験が行われている。
(<http://boinc.iaik.tugraz.at/>)

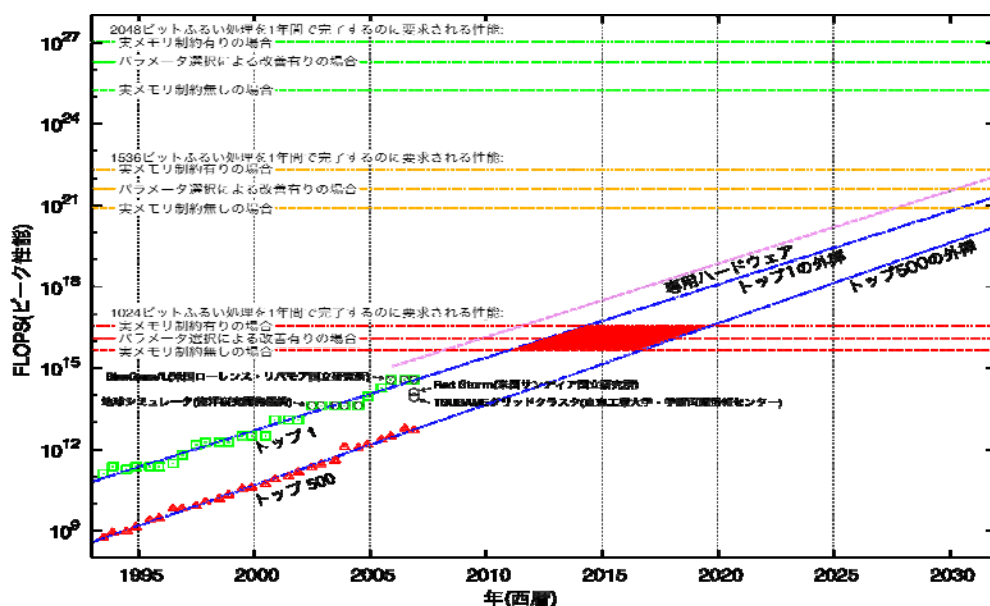


図 2 - 4 計算機性能の向上及びふるい処理計算量の予測

RSA暗号における鍵強度の低下の影響

- RSA暗号においては、素因数分解アルゴリズムに関する研究の進展又はコンピュータの計算速度の向上により、現実的な時間内に「公開鍵」から「秘密鍵」が解読されることで鍵の強度が低下する。
- 公開鍵暗号方式で「公開鍵」から「秘密鍵」が解読されることは致命的。
 - 利用者の署名を偽造できる(利用者の秘密鍵が漏えい)
 - にせもの電子申請、電子入札、電子申告・・・が可能(なりすまし)
 - これまで利用者が作成した電子署名つき文書の信頼性が喪失

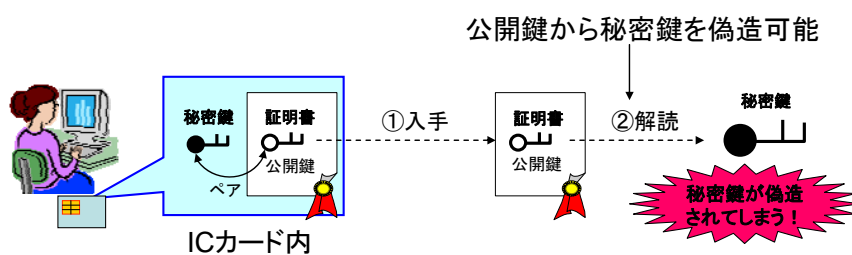


図 2 - 5

このようにして、仮にハッシュ関数の計算困難性や RSA 暗号の鍵強度が低下し、電子署名について否認することが可能となれば、それ以降に作成される電子署名が問題となるだけでなく、安全性が低下する前に電子署名が付された電子文書の信頼性も喪失する。

(4) 検討結果

○SHA-1、RSA1024bit を用いた新規電子署名の中止を見据え、指針第3条で規定する特定認証業務に係る電子署名の基準に、どのような電子署名の方式を追加すべきか

電子政府推奨暗号リスト（総務省・経済産業省、平成15年2月）では、既に、ハッシュ関数について注釈で「256ビット以上のハッシュ関数を選択することが望ましい」としており⁷、「暗号技術検討会2005年度報告書」において、SHA-1に代わる暗号として、SHA-2（SHA-256、SHA-384、SHA-512）が提案されている。また、RSA1024bitに代わる暗号については、第16回情報セキュリティ政策会議（平成20年2月4日）において、パブリックコメント案として決定された「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針(案)」(以下「政府機関情報システム移行指針(案)」という。)において、政府認証基盤に係るものとしてはRSA2048bitの利用が示されているところである。

以上を踏まえ、告示第3条（特定認証業務に係る電子署名の基準）に規定する特定認証業務に係る電子署名の基準においても、より安全性の高い暗号技術への移行を促すため、速やかにSHA-2を追加し、SHA-2及びRSA2048bitによる電子署名について行う認証業務も特定認証業務に含めることが適当である。

○SHA-1、RSA1024bit を用いた新規電子署名の中止を見据え、指針第3条で規定する特定認証業務に係る電子署名の基準からSHA-1、RSA1024bitを用いた電子署名の方式を削除することを含め、どのような措置をどのようなスケジュールで行うべきか。

(改正の時期及びそれまでに行うべき措置等)

電子署名法では、第3条の推定規定が司法の場で適用されやすくなることを期待しつつ、国民に対する認証業務の信頼性の目安になるものとして、特定認証業務⁸に対する認定制度を設けている。しかしながら、上述のように、電子署名で用いる暗号アルゴリズムの安全性が低下すれば、他人名義の電子署名を作出（なりすまし）することや電子文書を改ざんすることができるようになり、そのアルゴリズムを用いてされた電子署名が「本人だけが行うことができる電子署名」の要件や電子署名の定義自体を満たさなくなるため、特定認証業務の要件として施行規則第2条及び告示第3条においてSHA-1、RSA1024bitを用いた電子署名の方式を規定し続けることは適当ではない。

既に述べた、暗号技術検討会等による報告を踏まえれば、新たな攻撃手法に関する研究の進展によって急速に危殆化し得る暗号技術の一つであるSHA-1の電子文書への利用は停

⁷ 注釈の該当項全文は、「新たな電子政府システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りでない。」となっている。

⁸ 電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務

止すべきであると考えられるが、それに代替する環境がないまま、直ちに停止することはできない。RSA1024bitについても、今後数年で、相応の能力を有するコンピュータを用いれば1年間の計算によって攻撃可能となるため、SHA-1と同様により安全な暗号アルゴリズムへの移行が望まれるが、これについても代替環境の構築が必要である。

他方、官民間問わず、SHA-1及びRSA1024bitによる電子署名に係る認証基盤及びアプリケーションシステム等については、SHA-2及びRSA2048bitへの移行に当たり、その用途に応じたリスク、コスト、システム更改時期等を考慮することとなる。認証基盤及びアプリケーションシステムの相互運用性を確保しつつ電子署名の円滑な利用を確保する観点からは、関係者が一定の期間内に移行することが望ましい。関係者の準備期間を考慮すれば、SHA-1及びRSA1024bitの利用を停止すべき時期を含め移行期間が予め示されることが必要と考えられる。

また、認定認証事業者の中には政府認証基盤（GPKI）と相互認証を行っている事業者が多く存在するため、暗号アルゴリズムの移行に際しては電子政府システムの移行状況と歩調を揃えた対応が必要である。そこで、主務省においては、政府機関情報システム移行指針(案)も踏まえ対応を行っていくことが適当である。

SHA-1及びRSA1024bitの利用を停止すべき時期について、既に述べた事項も含め、考慮すべき要素をまとめると、以下のようになる。

一 SHA-1は、電子署名のアルゴリズム中に利用されており、電子文書への電子署名においては、複数レベルの脅威が想定される。

- ・電子署名が無い複数の異なる文書に同一の電子署名が付される脅威（衝突計算攻撃）

- ・電子署名が付された電子文書と同一の電子署名が別の電子文書に付される脅威（第二原像計算攻撃）

衝突計算攻撃に要する時間の推定に関しては、2006年6月時点において、国内最高速のスーパーコンピュータを用いれば462年以下で衝突発見されるおそれがあることが示されている。一方、第二原像計算攻撃に関しては、現時点において報告されていない。

電子署名法は、電子文書に付す電子署名に紙文書における署名と同等の推定効を与える法律であるので、電子署名者による否認を防止できること及び電子署名の信頼性を技術的に確保する必要がある。このためには、第二原像計算攻撃による脅威のみならず、衝突計算攻撃による脅威も含めて想定する必要がある。

衝突計算攻撃による脅威は、2015年前後には現実的になることが想定される（図2-3）ので、念のため、より安全性（衝突発見困難性）の高いアルゴリズムに移行することが望ましいこと。

二 RSA1024bitについては、概ね2015年以降に、危殆化のおそれが高まってくることを示されている（図2-4）こと。

三 政府機関情報システム移行指針(案)において提示されている、政府機関の各情報システムを新暗号アルゴリズムへ適応させる時期は2013年度までであること。（注：政府機関情報システム移行指針(案)は、3月7日を締切日としてパブリックコメントの募集が行われており、その状況によってはこの提示どおりとはならない可能性がある

る。)

したがって、これらの要素及び電子証明書の有効期間を勘案すれば、SHA-2 及び RSA2048bit による電子署名についての特定認証業務の認定は遅くとも 2014 年度早期までに行うことが必要である。

なお、政府認証基盤と相互認証している認定認証事業者が多いことから、当該認定認証事業者が SHA-2 及び RSA2048bit による電子署名について行う特定認証業務について速やかに政府認証基盤に相互認証の申請を行えるようにするためには、当該認証事業者に対して変更認定のための調査が必要である場合は、あらかじめ 2013 年度に行っておくなどの工夫を要する。

これらの措置を前提に、電子署名法施行規則及び告示において、SHA-1、RSA1024bit を削除する時期は、可能な限り 2014 年度末前後（主務大臣が SHA-2 及び RSA2048bit による電子署名について行う特定認証業務に対する認定を完了し、認定認証事業者が利用者に対する SHA-2、RSA2048bit による電子証明書の発行を終えた後）とすることが妥当である。

したがって、主務省においては、図 2-6 のスケジュール案を基本として、制度改正作業等を進めていくことが適当である。

ただし、これはあくまで SHA-1、RSA1024bit の急速な危殆化を前提としていないものであり、状況によっては、緊急的措置（コンティンジェンシープランの発動）が必要である。今後主務省は、暗号技術検討会等の意見等を踏まえ、早急にコンティンジェンシープランを作成し、暗号の急速な危殆化に備えるべきである。

なお、上述のように、暗号アルゴリズムの移行に当たっては、認証事業者のほか、機器ベンダ、SI 事業者及びエンドユーザ等に対しての、コストやシステム更改のタイミング等を含めた影響を十分に考慮し、関係者相互の合意形成を図りながら進めていくことが必要である。

（施行規則の改正と電子署名法 3 条による推定効の関係の整理）

電子署名法第 3 条は、電子文書の真正な成立の推定効を規定するものであることから、適用の場面として、電子文書が作成された時点から一定期間を経過した後に当該電子文書の成立の真正性が争われる場合が想定される。すなわち、①電子文書に電子署名がされた時、②その電子署名が電子証明書及びその失効に関する情報により検証された時、③後日当該電子文書の成立の真正性が争われる時、という時間の経過の中で、電子署名がその方式に応じて本人にしかできないものであったかどうかの問題となり得る（電子証明書による検証は、電子証明書の有効期間中に行われることが予定されている、検証結果については、必要に応じ、後日の利用に備えて適切に保管される必要がある。）。

したがって、電子署名をした時においては当該電子署名が電子署名法第 2 条第 3 項に規定する特定認証業務の要件を満たしていたが、電子文書の真正な成立が問題となる時点において、電子署名で用いる暗号アルゴリズムの安全性が低下することにより当該電子署名

が特定認証業務の要件を満たさないものとなっていた場合の適用関係が問題となり得る。

もとより、電子署名法第3条の推定効が適用される電子署名は、第2条第3項の特定認証業務の対象となる電子署名と必ずしも一致するものではないが、特定認証業務の認定制度が、認定を受けた認証業務に係る電子署名について電子署名法第3条の推定規定が適用されやすくなることを期待して設けられた背景に鑑みれば、電子署名法第2条第3項に規定する主務省令を改正することにより特定認証業務の対象となる電子署名の範囲を変更するに当たっては、変更の前後における電子署名法第3条の適用関係に関する考え方や特定認証業務の認定の効果を利用者及び署名検証者や裁判官が理解できるよう示す必要があるものと考えられる。

また、上述の変更にあたっては、適用関係の問題を回避するための技術的方策（例えば、特定認証業務の対象となる電子署名の範囲を縮小する改正の場合には、対象から外れる電子署名が付された電子文書について、変更後も特定認証業務の対象であり続ける電子署名を変更前に予め追加的に付しておく（この場合の署名者は、元の電子文書の署名者に限られない。）ことで元の電子文書の成立の真正性を担保する方法等）や、管理的方策（例えば、電子署名を付した電子文書を電子署名法第2条第3項に規定する主務省令の改正前から成立の真正性を確認する時点まで第三者機関等に預託し、改変等が行われていないことを証明する方法等）についても、併せて検討する必要があるものと考えられる。

これらの問題は、関係者間の十分な検討と調整を経る必要がある問題であるが、その一方で、利用者が対策を検討する十分な時間を確保することができるよう、電子署名法第2条第3項に規定する主務省令の改正に先立ち、前広に、利用者に広報されるべき問題であることから、早い段階で検討が開始されることが必要である。

（今後の検討事項）

以上の移行を円滑に進めるため、主務省及び関係者により、以下の事項について更に調査検討を行うことが適当である。

- ・影響範囲の詳細な検討（検証アプリケーション、HSM⁵、ICカード、電子署名付き文書、電子証明書）
- ・詳細な移行手順の策定（暗号技術検討会等との連絡手順を含む）
- ・電子証明書の運用方法（発行者署名検証符号に係る電子証明書の値を変換するハッシュ関数の扱いを含む）
- ・電子署名付き文書に対する対策（例：再署名、タイムスタンプ、長期署名方式等）
- ・制度面の課題（推定効への影響、認定の効果、失効の判断基準）
- ・一般利用者を含む関係者への周知方法

⁵ HSM(Hardware Security Module)：公開鍵暗号の鍵ペアや、共通鍵暗号の鍵を生成する機能及びそれらの鍵を保管する機能を有する装置。物理的な攻撃に対して耐性（耐タンパー機能）を有する。

2008 年度 早期	暗号アルゴリズムの移行に向けた具体的な検討の開始、特定認証業務に係る電子署名の基準に SHA-2 を追加。
(2010 年度)	(政府機関システム暗号移行開始) *政府機関システム移行指針(案)による
(2013 年度)	(政府機関システム新旧暗号アルゴリズム (SHA-1 及び SHA-2、RSA1024bit 及び 2048bit) 対応環境構築が完了) *政府機関システム移行指針(案)による
2013 年度末 まで	認定認証事業者に対して、暗号移行に係る変更認定のための調査が必要な場合は実施し、認定認証事業者は、RSA2048bitを用いた発行者鍵ペア ⁶ を新たに生成する必要がある場合は、生成。
2014 年度 早期まで	認定認証事業者は、RSA2048bit による発行者鍵ペアを活性化させ SHA-2 及び RSA2048bit による電子署名についての認証業務を開始。
2014 年度 末前後を目 途	SHA-1、RSA1024bit による利用者電子証明書の有効期間後に、特定認証業務に係る電子署名の基準から、SHA-1、RSA1024bit を削除。 (SHA-1、RSA1024bit による利用者電子証明書の有効期間について、各認定認証事業者は、SHA-2、RSA2048bit による利用者電子証明書への切替を考慮し、あらかじめ調整を図ること等が求められる。)

図 2 - 6

⁶ 発行者署名符号と発行者署名検証符号のペア。

2. 認定認証業務における利用者の真偽の確認について（制度的論点）

（1）論点

認定認証業務において、電子証明書の発行に際して行うこととされている利用申込者の真偽の確認方法については、図2-7に示された方法のみが認められているが、現行の方法に加え、他の代替する真偽の確認方法を認めることはできないか。

（2）検討すべき事項

- ・利用者の真偽の確認方法について、施行規則第5条第1項本文の「住民票の写し、戸籍の謄本若しくは抄本、外国人登録法第4条の3に規定する登録原票記載事項証明書又はこれらに準ずるもの」の提出を求めることに代替する方法を認めるとする施行規則の改正を行うことは可能か。
- ・上記が可能であるとした場合、認定認証事業者である全国社会保険労務士会連合会、日本税理士会連合会、日本司法書士会連合会及び日本土地家屋調査士会連合会（以下「士業4団体」とする。）は、各士業関係法に基づき整備された名簿を管理しているが、これらの名簿の利用をもって上記の代替する方法とすることはできないか。

（3）背景

・現在の電子署名法における利用者の真偽の確認方法（施行規則第5条）

認定認証事業者が新規に電子証明書を発行する場合における利用者の真偽の確認方法については、法第6条第1項第2号の規定に基づき、施行規則第5条第1項に規定されている。

施行規則第5条第1項の規定は、電子証明書を新規に発行する場合において認定認証事業者が最低限行うべき利用者の真偽の確認の方法を規定するものであり、同項第1号は、利用の申込みをする者に係る「住民票の写し、戸籍の謄本若しくは抄本、外国人登録法第4条の3に規定する登録原票記載事項証明書又はこれらに準ずるもの」（以下これらを「必要的提出書類」という。）の提出を求めた上、同号イからニまでに規定する方法のうち少なくとも1以上の方法（以下「本人確認方法」という。）により利用申込者の真偽の確認を行うものでなければならないとしている。

本人確認方法については、同号ニにおいて、「イ、ロ又はハに掲げるものと同等なものとして主務大臣が認めるもの」と規定されているが、これは、同号イからハマまでの方法以外にも、各業界において培われた様々なビジネスモデルが存在し得るところ、そのようなものについても、同号イからハマまでに掲げる方法と同程度に利用

者の真偽を確認することが可能であると認められる場合には、法が規定する基準を満たすものとして評価されることがあり得ることを前提としている。

一方、施行規則第5条第1項本文の必要的提出書類については、これを提出することが必須であり、他の手段によることは認められていない。

(参考) 認定認証業務における利用者の真偽確認方法について

●タイプ1(電子署名及び認証業務に関する法律施行規則第五条第一項第一号)

住民票の写し or 戸籍の謄本若しくは抄本 or 外国人登録原票記載事項証明書の提出

※「これらに準ずるもの」として、住民票記載事項証明書 or 外国人登録原票の写しも可

タイプ1-A	タイプ1-B	タイプ1-C
<ul style="list-style-type: none"> ・旅券 ・別表(※)に掲げる官公庁が発行した免許証等 ・外国人登録証明書 ・写真付き住民基本台帳カード ・官公庁等の職員証明書で写真付きのもの <p>のうちいずれか1以上の提示</p> <p>※例：運転免許証、船員手帳、海技免状、小型船舶操縦免許証、戦傷病者手帳、宅地建物取引主任者証、電気工事士免状、無線従事者免許証、認定電気工事従業者認定証等</p>	<p>利用申込書に押印した印鑑に係る印鑑登録証明書の提出</p> <p>※これと「同等なもの」として、在日外国公館(大使館、領事館等)が発行するサイン証明書の提出も可</p>	<p>本人限定受取郵便(※以下(1)~(4)のいずれかの方法で本人確認を行うものに限る)により申込みの事実の有無を照会し、これに対する返信を受領する方法</p> <p>(1) タイプ1-Aに掲げる書類のうち1以上</p> <p>(2) 健康保険等の被保険者証、国民年金手帳、国民年金等の年金証書、共済年金等の証書のうち2以上</p> <p>(3) (2)のうち1以上及び学生証、会社の身分証明書又は公の機関が発行した資格証明書(タイプ1-Aに掲げるものを除く)で写真付きのものうち1以上</p>

※上記書類を必須提出物とし、かつ、以下の3タイプのうち1つを選択

●タイプ2(電子署名及び認証業務に関する法律施行規則第五条第一項第二号)

公的個人証明書に係る電子署名により真偽確認を行う方法

●タイプ3(電子署名及び認証業務に関する法律施行規則第五条第二項)

タイプ1又は2による真偽確認を行って発行された電子証明書に係る電子署名により真偽確認を行う方法

図 2 - 7

・士業4団体の要望

認定認証事業者でもある士業4団体は、各士業関係法に基づき整備された名簿を管理しており、認定認証業務における利用者の真偽の確認にこれらの名簿を利用可能とすることについて要望している。また、電子政府評価委員会においても、同様の指摘がされている。

(4) 検討結果

○利用者の真偽の確認方法について、施行規則第5条第1項本文の「住民票の写し、戸籍の謄本若しくは抄本、外国人登録法第4条の3に規定する登録原票記載事項証明書又はこれらに準ずるもの」の提出を求めることに代替する方法を認めるとする施行規則の改正を行うことは可能か。

法が認定認証業務の制度を設けた趣旨は、一定の技術的信頼性と認定の基準における

利用者の真偽の確認の信頼性により、この業務による証明があれば、当該証明に係る電子署名がされた電磁的記録については、法第3条の推定が働きやすくなることを期待したものである。

したがって、仮に、代替する方法を認める場合であっても、現行の利用者の真偽の確認と同等のレベルの実質が確保される必要があることはいうまでもない。

現行の制度が、必要的提出書類の提出を求める目的は、公的な機関が証明する利用者の氏名、住所及び生年月日をもって利用者の実在性を確認し、一意に特定することにあると考えられる。

また、これらの必要的提出書類は、一定の時点における登録事項を証明するものであって、その有効期間が定められておらず、また、施行規則第5条第2項の規定により少なくとも5年間に一度の頻度で真偽の確認を行うことが求められているにとどまることに鑑みれば、必要的提出書類によって得られるべき情報は、必ずしも真偽の確認の時点における最新のものであることを要しないものと考えられる。

したがって、利用者の氏名、住所及び生年月日等の情報を確認することができる資料があり、この資料の作成根拠が法令に定められているなど、当該資料が一定の信頼性を有していると認められるものである場合には、利用者の実在性を確認し一意に特定するための手段としてこれらの資料を用いることをもって必要的提出書類の提出に代えることとする施行規則の改正も十分考慮に値するものであると考えられる。

なお、当該資料が一定の信頼性を有していると認められるものであるということが出来るためには、利用者の氏名等の情報が住民票の写し等の公的書類に基づいて記録されるものであること、記録された事項の変更・更新等が一定の場合に行われるべきであること等が法令等に規定されている必要がある。

○認定認証事業者である士業4団体は、各士業関係法に基づき整備された名簿を管理しているが、これらの名簿の利用をもって上記の代替する方法とすることはできないか。

士業4団体は、それぞれ認定認証事業者として業務を行っているが、その発行する電子証明書は、各々の各士業関係法に基づき登録業務を行うこととされている名簿に登録された会員のみをその発行の対象としている。

これらの名簿には、会員の氏名、住所及び生年月日等が記録されているが、これらの記録は登録時に会員から提出される資格を証する書面及び住民票の写し等の公的書類により行われるものであることが各士業関係法令等に規定されているほか、登録事項の変更、取消し等の手続についても同様に法令に規定されている。

したがって、仮に、当該名簿の根拠となる法制度や運用・管理等の実態が電子署名法の趣旨に沿うものであるならば、利用申込者が法律の規定に基づく士業団体の名簿に登録された者であり、かつ、申込みを受けた認定認証事業者が当該名簿の登録を行う者である場合において、当該名簿に記録された事項を確認する方法について、必要的提出書類の提出を求めることに代替する方法として認めることも可能であると考えられる。

主務省は、前記の方法を実施するため、平成 20 年度中に施行規則を改正することを目途に検討を進めていく必要がある。検討に当たっては、士業 4 団体の名簿の根拠となる法制度や運用・管理等の実態が電子署名法の趣旨に沿うものとなっていることを確認する必要があるほか、電子署名の普及促進の観点から、これらの名簿以外のものについても、法の趣旨を損なわない範囲において利用者の真偽の確認に用いることが可能となるような施行規則の改正をも考慮すべきである。また、同様の観点から、主務省は、本人確認方法について、施行規則第 5 条第 1 項第 1 号ニの規定を積極的に活用するよう努めるべきである。

3. 普及促進策について（ビジネス的論点）

（1）論点

電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進、それによる国民生活の向上、国民経済の健全な発展に寄与することが電子署名法の目的であり、電子署名法第 33 条及び第 34 条の主旨にのっとり、国は、特定認証事業者やその利用者に対する援助、電子署名に係る広報活動等を行いつつ、必要があればその他の方策も検討するなどして、電子署名を一般化させる工夫が必要ではないか。

（2）検討すべき事項

電子署名を身近なものとするためには、電子署名の利用場面、電子署名の認知度を踏まえ、電子証明書の取得・利用に係る国民・企業等の負担を軽減するとともに、電子署名を用いた場合のメリットを明確にすべきである。そのためにとるべき普及促進策の方向性は、どのようにあるべきか。

（3）背景

- 1) 電子政府システムにおける電子署名の利用は、電子入札、電子申請、電子申告を中心に拡大している。
- 2) 民間においては、電子契約、電子文書保存などに利用され始めている。
- 3) 認定認証事業者に対する指定調査機関による調査については、認定認証事業者の負担軽減のため、より効果的・効率的なものとなることが期待されている。

（4）検討結果

電子政府システムや民間の電子商取引等において国民・企業等による電子署名の円滑な利用を確保するためには、電子証明書を発行する認証事業者の役割が重要であり、特定認

証業務の認定制度は一定の役割を果たしてきている。このため、電子証明書発行枚数増加によるスケールメリットに期待して、電子署名の利用場面や潜在的ニーズも踏まえ、官民が協力して我が国における電子署名の社会的認知度を向上させていくことにより、電子署名のより一層の普及促進、認証ビジネスの成立及び認定制度の安定的な運用を同時に推進していく取組が必要である。

また、電子証明書の取得・利用に係る国民・企業等の負担を軽減するとともに、電子署名を用いた場合のメリットを明確にすることも必要である。

なお、このような観点から、現在の法制度に改善すべき点があれば、可及的速やかに改善しつつ、電子署名の一層の普及促進策を実施すべきである。

上記を踏まえ、主務省においては、関係者とも協力して以下のような普及促進策を実施・検討していくことが適当であり、その具体については、今後主務3省を中心に、引き続き、電子署名法の目的である国民生活の向上及び国民経済の健全な発展に寄与することを踏まえ、諸外国の事例等も参考にしつつ検討を進めていくべきである。

◎新たな取組の検討例

- ・ 指定調査機関の調査を受ける認定認証事業者の負担を更に軽減するため、調査に当たって既に調査対象（設備、業務方法）が外部監査を受けている場合に、当該監査結果の一部を活用することにより指定調査機関による調査の工数を削減できるかどうかについて検討を行う。
- ・ 電子署名法の解釈を示すガイドライン等を作成し、認証事業者及び国民に向けて公開
- ・ 有用なアプリケーションの利用を前提とした新たな利用分野を含む利用事例の普及（企業、公的分野等）
- ・ 電子署名への理解促進を図るために電子署名を擬似的に体験利用できるツールの開発
- ・ 認定認証事業者が発行する電子証明書の利用申込受付方法の多様化（代理人申込の普及など）

◎電子署名法第33条及び第34条に基づき従来から行っている各種の普及促進策の継続的实施

- ・ 各種情報提供及び広報活動
 - － 企業・個人を対象とした電子署名の利用方策に係るセミナーの開催
 - － 電子署名及び認証業務への理解促進を目的とした、
 - － Web ページの充実
 - － パンフレットの配布、
 - － ポスターの掲示 等

◎公的個人認証サービスとの連携（認定認証事業者等が必要とする実在性確認を担保するトラストアンカー（信認の原点）の提供元として公的個人認証サービスを利用）

4. その他の諸課題

(1) 認定認証業務の電子証明書の発行対象

■ 課題

自然人だけでなく、法人名や役職名等を対象とする電子証明書を発行する認証業務についても、電子署名法に基づく認定を受けられるようにできないか。

■ 考え方

わが国の商慣習にかんがみて、例えば書面（紙）での契約等において、当該契約の責任者・担当者等の氏名なしに会社印・役職印のみで契約等を行うことは一般的ではない。電子署名は、電子の世界において、手書き署名及び押印に相当する位置付けである。電子署名について、手書き署名・押印と同等の法的取扱いを定める電子署名法においては、認定の対象は自然人を電子証明書の発行対象とする特定認証業務とするのが妥当である。

その一方で、電子署名法は、認定認証業務以外の認証業務において法人名や役職名を電子証明書の発行対象とすることを何ら妨げていない。同法第 34 条では、国が、認定認証業務に限定することなく、電子署名及び認証業務一般に関する教育活動、広報活動等を行うよう努めるべきことが定められており、主務省においては、認定認証業務以外の認証業務においてニーズを踏まえた多様なサービスが展開されることを、支援していくべきであると考えられる。

なお、本件課題が指摘されている背景には、法人における各種業務の一環で電子署名が必要となるところ、電子証明書の発行申請において、当該電子署名を実施する者個人の負担を軽減し、かつ、当該電子署名が法人の各種業務の目的で実施されたということを明らかにしておきたいといったニーズなどがあるのではないかと考えられる。このようなニーズについては、例えば、電子署名を行おうとする者に代わって、代理人が認証業務の利用申込み等を行うことなどが対策として考えられる。このような申し込みは、法制度上は可能となっているが、実際には、そのようなサービスを行っている認定認証業務は現在存在しない。主務省は、このような事例について、その要因をよく分析し、必要な改善及び支援策について引き続き検討していくべきである。

(2) 認定認証業務の電子証明書に記載する属性情報

■ 課題

特定認証業務の認定制度においては、電子証明書に記載する氏名・住所・生年月日以外の属性についての証明は認定対象となっていないが、認定対象とすることができないか。

■ 考え方

属性に関する証明は当該属性を決定している者（会社における役職においては会社代表、士業資格においては士業団体等）が属性を証明する権能を持っていること等によって生じると解釈することが一般的である。電子署名法規則第6条第8号において、氏名・住所・生年月日以外の属性についての証明が認定認証業務に係るものであるとの誤認を防止する措置が求められている趣旨は、本来属性が、それを証明する権能を有する者によってしか証明され得ないものであるにもかかわらず、認定認証業務の電子証明書に異なる記載がある場合に、その属性についてまで氏名等と同じレベルの推定効が働く可能性があるとの誤認を生じさせないようにするためである。認定認証業務の電子証明書に属性を記載することが否定されているわけではない。

したがって、認定認証業務が属性の確認に用いている情報が属性を証明する権能を持った者から正確に提供されていることが確認されれば、認定認証業務による電子証明書に記載された属性情報に関する事実上の推定が働くと期待される。なお、その際の課題の有無を確認するとともに、属性についての証明を認定対象とすることができないかについては、引き続き、社会ニーズを踏まえ、検討を行うことが適当である。

（3）電子署名の長期検証性の確保

■ 課題

電子署名は、対応する電子証明書の有効期間が過ぎると、通常の方法ではその有効性を検証することができなくなる。電子署名法においても、電子文書を長期保存する場合の電子署名の利用を想定し、電子署名の長期検証性の確保について規定を置くべきではないか。

■ 考え方

電子署名法は、電子署名の法的取扱いを確立することを目的としており、これに関し必要な事項を定めるものである。電子署名をどのように利用するかについては、市場の活動を制限しないという観点からも特に規定しておらず、電子文書の長期保存に利用する場合の措置に関する規定を置くことも考えにくい。しかしながら、電子署名をとりまく環境の整備という視点から、主務省は、電子署名の長期検証を可能とする各種技術の開発・標準化等を支援していくことが適当である。

（4）認定制度の複数レベル化

■ 課題

認証業務の認定制度に、複数の認定レベルを設けることはできないか。

■ 考え方

電子署名法は、我が国の情報化推進のために不可欠な基盤整備として、電子署名に署

名・押印と同等の取扱いを認める必要があるということから立法されたものであり、署名・押印と同等の効力を認めるにふさわしい措置に限って推定規定を適用することが想定されている。推定規定が適用されやすくなることを期待して、本認定制度に、複数のレベルを設ける（二重底とする）ことは不適當であると考えられる。

ただし、国により認定された認証業務を行う者が、それ以外の認証業務を行うことは自由であり、後者の実施に当たって国は何ら直接的関与をしないものの、同一事業者が認定認証業務を行っていることにより得られる信頼感は少なくないものとする。

（５）利用者及び署名検証者による適切な電子署名の利用

■ 課題

電子署名法には、利用者（認証局から電子証明書の発行を受け、電子署名を行う者）及び署名検証者に対する義務的規定は存在しないが、利用者がどのようなレベルの管理を行えば電子署名法第3条における「適正」な管理と考えられるかについて、何らかの指針等が必要ではないか。

■ 考え方

特定認証業務利用者等への援助に関する主務大臣の努力義務を定めた電子署名法第33条、電子署名及び認証業務に対する国民の理解を深める活動についての国の努力義務を定めた第34条の観点から、利用者、署名検証者が正しい理解のもと、円滑に電子署名を利用できるよう、適正な秘密鍵の管理等のあり方について検討を行った上、必要な広報活動を行っていく。

（６）認定認証業務間でのブリッジ認証局の構築

■ 課題

認定認証業務間でのブリッジ認証局（BCA）を構築して、認定認証業務に係る電子証明書の相互運用を促進するべきではないか。

■ 考え方

必ずしもすべての認定認証事業者が、他の認定認証事業者との相互運用を望んでいるわけではなく、国が認定認証業務間のBCAの構築に積極的に関与する必要はないが、認定認証事業者の自主性において民間BCAを構築する際は、国は適切に情報提供等を行うべきである。

電子署名及び認証業務に関する法律の施行状況に係る検討会

構 成 員・オブザーバ名簿

(構成員)

石黒 義昭	株式会社コンストラクション・イーシー・ドットコム 代表取締役常務
澁谷 裕以	社団法人日本経済団体連合会情報通信委員会情報化部会 IT ガバナンス WG 委員
高橋 伸和	日本ベリサイン株式会社 顧問
辻井 重男	情報セキュリティ大学院大学 学長
手塚 悟	株式会社日立製作所システム開発研究所情報サービス研究センタ シニアマネージャ
西村 達之	セコムトラストシステムズ株式会社 代表取締役副社長
早貸 淳子	情報セキュリティ大学院大学セキュアシステム研究所 客員研究員
藤原 宏高	日本弁護士連合会コンピュータ委員会 委員
松本 恒雄	一橋大学大学院法学研究科 教授
満塩 尚史	ディーディーエヌコンサルティング株式会社 ディレクター

(オブザーバ)

伊藤 毅志	内閣官房情報セキュリティセンター 参事官
亀田 繁	財団法人日本情報処理開発協会電子署名・認証センター センター長
塚田 桂祐	総務省大臣官房 参事官
中井川 禎彦	総務省行政管理局行政情報システム企画課情報システム 管理官
山内 徹	内閣官房 IT 担当室 内閣参事官

(敬称略・五十音順)

電子署名及び認証業務に関する法律の施行状況に係る検討会 開催要綱

1 目的

「電子署名及び認証業務に関する法律」(以下「電子署名法」という。)は、平成 12 年第 147 回国会の審議を経て、同年 5 月に公布、平成 13 年 4 月 1 日に施行された。

電子署名法附則第 3 条においては、施行後 5 年を経過した場合に、同法の施行の状況について検討を行うものとされており、総務省、法務省及び経済産業省は、平成 18 年度以降、外部有識者のヒアリングを行うなどして同法施行上の課題の抽出等を実施してきた。この検討会は、当該抽出した課題について議論を行い、今後の電子署名法の運用に反映していくため、開催するものである。

2 名称

本検討会は、「電子署名及び認証業務に関する法律の施行状況に係る検討会」(以下単に「検討会」という。)と称する。

3 検討事項

- (1) 電子署名に用いる暗号技術の安全性向上に係る方策について
- (2) 認定認証業務における利用者の真偽の確認について
- (3) 特定認証業務の認定制度の運用について
- (4) その他検討が必要な事項

4 構成及び運営

- (1) 本検討会は、総務省政策統括官(情報通信担当)、法務省民事局長及び経済産業省商務情報政策局長の検討会として開催する。
- (2) 検討会の構成は、別紙のとおりとする。
- (3) 検討会には、座長及び座長代理 1 名を置く。
- (4) 座長は、構成員の互選により定める。
- (5) 座長は、検討会構成員の中から座長代理を指名する。
- (6) 座長は、検討会を召集し、主宰する。
- (7) 座長は、必要に応じ、関係者等の出席を求め、意見を聞くことができる。
- (8) その他、検討会の運営方法は、座長が定めるところによる。

5 開催期間

平成 19 年 12 月から平成 20 年 3 月末を目途に計 3 回程度の開催を予定するが、必要に応じて延長する。

6 庶務

本検討会の開催にあたっては、総務省情報通信政策局情報流通振興課、法務省民事局商事課及び経済産業省商務情報政策局情報セキュリティ政策室が共同して庶務を担当する。

電子署名及び認証業務に関する法律の施行状況に係る検討会
開催状況

開催時期	主な議事
第1回 (平成19年12月18日)	○電子署名法の施行状況について ○電子署名法検討会の検討事項について ○その他の諸課題について ○今後の進め方について
第2回 (平成20年2月19日)	○諸外国の事例について ○報告書素案（パブリックコメント案）について
第3回 (平成20年3月31日)	○暗号技術検討会からの回答について ○報告書案（パブリックコメント案）に係る御意見への対応 ○報告書案について

外国の事例

項目	韓国（公認証明書）	（参考）日本（認定認証業務）	（参考）日本（公的個人認証サービス）
1. 人口	4700 万人	1 億 2800 万人	同左
2. 開始時期	1999 年	2001 年 4 月	2004 年 1 月
3. 電子証明書の発行枚数	1380 万枚（2006 年 10 月）	31 万 4 千枚（2007 年 3 月末） ※認定認証業務に係るもの。	45 万枚（2008 年 1 月末）
4. 電子証明書の用途	署名、認証	署名	署名
5. 形態	1 枚の証明書を署名用と認証用の用途に使用	署名用のみしか存在せず	署名用のみしか存在せず
6. 電子証明書の格納媒体	・パソコンのハードディスク、USB メモリ、フロッピーディスク、CD-ROM、IC カード、携帯電話の本体メモリ	IC カード、USB トークン、携帯電話等（規定無し）	住民基本台帳カードその他の総務省令で定める電磁的記録媒体
7. 電子証明書の発行機関	・原則、国に認可された官民の機関（2007 年 3 月現在 6 機関） ※公認を受けない認証機関が証明書を発行することは禁じられてはいないが、その利用範囲は実際には制限を受ける。	・認定認証事業者（2008 年 2 月現在 17 社 19 業務） ※認定を受けていない認証事業者が電子証明書を発行することは可能。	都道府県
8. 電子証明書の発行手続	認証局又は登録局の窓口で実在性確認／本人確認後、サイト上で発行	実在性確認／本人確認の方法については、制度上、複数の選択肢がある（窓口、郵送、オンライン）	居住地の市区町村窓口で実在性確認／本人確認後、住民基本台帳カードに格納
9. 電子証明書のオンライン発行	可能（登録局でオンラインバンキングサービス等の申込時に既に本人確認を行っている場合）	公的個人認証サービスの電子証明書により可能	不可

10. 電子証明書の更新 手続	既存の公的電子証明書を 用いたオンライン更新のみ	基本的には新規発行時 と同様の手続	新規発行時と同様の手 続
11. 電子証明書のオン ライン更新	可能	利用者が現に有してい る認定認証業務の電子 証明書により可能（公 的個人認証サービスの 電子証明書によっても 可能）	不可
12. 電子証明書の有効 期間	1年	5年を超えない	3年
13. 電子証明書の発行 手数料	無料（用途限定）、4,400 ウォン（一般用）	認定認証事業者ごとに 異なる	500円
14. 電子証明書を利用 したサービス	<ul style="list-style-type: none"> ・各種行政サービスの申請 ・住民情報データベースへのアクセス（ログイン） ・オンラインバンキング ・オンライン株取引 ・クレジットカード決済等 	<ul style="list-style-type: none"> ・電子申請 ・電子入札 ・電子契約 ・電子公証等 	各種行政サービスの申 請
15. 利用者へのインセ ンティブ	<ul style="list-style-type: none"> ・行政サービスにて手 数料の割引 ・税金の払い戻し 	－	所得税の電子申告時 における税金の一部控除
16. 利用の義務化	<p>具体的なサービスで義務化</p> <ul style="list-style-type: none"> ・オンラインバンキング ・オンライン株取引 ・オンラインショッピング（クレジットカードによる10万ウォン以上の決済） 	<p>なし</p> <p>※ 認定を受けた認証業務であることが民間認証局の政府認証基盤との相互認証の条件となっている。</p>	なし
17. PKI に関わる法制度	<ul style="list-style-type: none"> ・電子署名法 ・公認認証局の施設設備基準に関する告示 ・CPS ガイドラインに関する告示 ・公認認証局が採用する安全対策に関する告示 ・実在性確認及び本人確認に関する告示 	<ul style="list-style-type: none"> ・電子署名法等 	<ul style="list-style-type: none"> ・公的個人認証法 ・認証業務及びこれに付帯する業務の実施に関する技術基準

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第7回」資料3-1「公的電子証明書に関する海外事例」
(http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kojin_ninsho/pdf/071211_2_si3-1.pdf)
- 「韓国における電子署名の利用」
(NTT データ、http://e-public.nttdata.co.jp/f/repo/381_a0605/a0605.aspx)
- <http://www.hikorea.go.kr/pt/>等