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

目次

主な略称一覧

略称	名称
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（平成 14 年 12 月 13 日法律第 153 号）
施行令	電子署名に係る地方公共団体の認証業務に関する法律施行令（平成 15 年 9 月 12 日政令第 408 号）
施行規則	電子署名に係る地方公共団体の認証業務に関する法律施行規則（平成 15 年 9 月 29 日総務省令第 120 号）
技術的基準	認証業務及びこれに附帯する業務の実施に関する技術的基準（平成 15 年 12 月 3 日総務省告示第 706 号）
電子署名法	電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号）
電子署名法指針	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 4 月 27 日総務省・法務省・経済産業省告示第 2 号）
電子署名法の施行状況に係る検討会	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
電子署名法の施行状況に係る検討会報告書	「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）
移行指針	「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」（平成 20 年 4 月 22 日情報セキュリティ政策会議決定）
住基カード	住民基本台帳カード
新電子証明書	SHA-256 及び RSA2048 による電子証明書
旧電子証明書	SHA-1 及び RSA1024 による電子証明書

1. はじめに

公的個人認証サービスは、第三者による情報の改ざんの防止及び通信相手の確認を行う高度な個人認証機能を、全国どこに住んでいる人に対しても安い費用で提供するサービスである。近年、公的個人認証サービスにおいて利用されているハッシュ関数[1]SHA-1 及び公開鍵暗号方式[2]RSA1024 について、暗号技術検討会[3]等において安全性の低下により将来問題が生じる可能性が指摘されている。当該指摘も踏まえ、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[4]（以下「電子署名法の施行状況に係る検討会」という。）において、電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号。以下「電子署名法」という。）に関する暗号アルゴリズム[5]の移行等について報告書（「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。以下「電子署名法の施行状況に係る検討会報告書」という。））が取りまとめられ、情報セキュリティ政策会議において政府機関の情報システムにおける暗号アルゴリズムの移行指針（「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」（平成 20 年 4 月 22 日情報セキュリティ政策会議決定。以下「移行指針」という。））が決定された。

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は、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についても有識者、地方公共団体、関係省庁等による検討を行い、公的個人認証サービスの安全性及び信頼性を引き続き確保することを目的として、平成 20 年 9 月 16 日から同年 12 月 18 日まで計 3 回開催された。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は、本検討会の検討結果として、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の必要性及び移行案、今後の検討事項等について取りまとめたものである。

---

1 与えられたデータから固定ビット長の値を生成する関数。（出典：移行指針 1 頁）

2 関連した 2 つの鍵（公開鍵と秘密鍵）を使用する暗号方式であり、一方の鍵（公開鍵又は秘密鍵）で暗号化したデータは他方の鍵（秘密鍵又は公開鍵）でのみ復号できるようになっている。2 つの鍵は、公開鍵が与えられても、秘密鍵を導き出すことが計算上困難な特性を持っている。（出典：移行指針 1 頁）

3 総務省大臣官房総括審議官及び経済産業省商務情報政策局長の研究会として毎年度開催。

4 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。

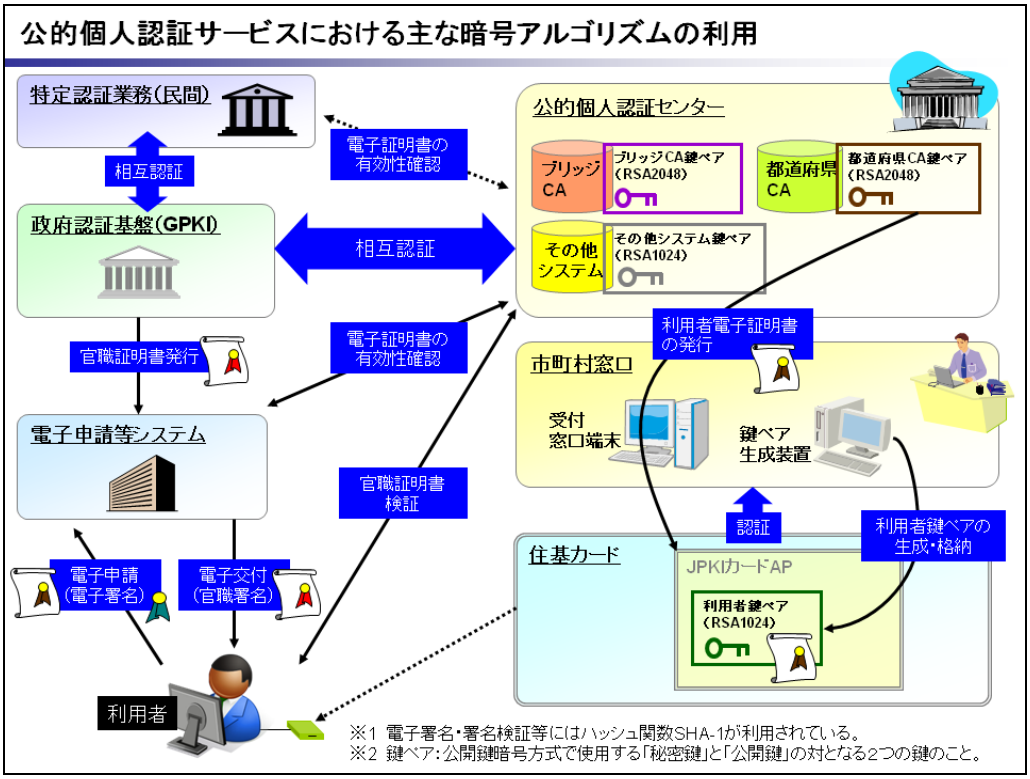
5 情報を暗号化する手順。

2. 公的個人認証サービスにおける暗号アルゴリズムの利用

2.1. 公的個人認証サービスにおける暗号アルゴリズムの利用

公的個人認証サービスにおいては、利用者が行う電子署名、電子証明書の発行に当たって都道府県知事が行う電子署名、署名検証者（行政機関等）が行う電子証明書の有効性確認、利用者が行う官職証明書の検証、鍵ペア生成装置及び受付窓口端末が正当なものであることの認証等に、SHA-1、RSA1024 等の暗号アルゴリズムを利用している。

図１　公的個人認証サービスにおける主な暗号アルゴリズムの利用



2.2. 公的個人認証サービスにおいて利用する暗号アルゴリズムを規定する法令等

公的個人認証サービスにおいて利用する暗号アルゴリズムについて、電子署名に係る地方公共団体の認証業務に関する法律（平成 14 年 12 月 13 日法律第 153 号。以下「法」という。）、電子署名に係る地方公共団体の認証業務に関する法律施行令（平成 15 年 9 月 12 日政令第 408 号。以下「施行令」という。）、電子署名に係る地方公共団体の認証業務に関する法律施行規則（平成 15 年 9 月 29 日総務省令第 120 号。以下

「施行規則」という。）並びに認証業務及びこれに附帯する業務の実施に関する技術的基準（平成 15 年 12 月 3 日総務省告示第 706 号。以下「技術的基準」という。）において、電子署名の基準及び利用者等が行う電子署名の方式、電子証明書の発行に当たって都道府県知事が行う電子署名の方式並びに特定認証業務を行う者に係る認定の基準を以下のとおり規定している。

○　電子署名の基準及び利用者等が行う電子署名の方式

法第 2 条第 1 項　この法律において「電子署名」とは、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）第 2 条第 1 項に規定する電子署名であって、総務省令で定める基準に適合するものをいう。

施行規則第 2 条　法第 2 条第 1 項に規定する電子署名に係る基準は、電子署名の安全性がほぼ同じ大きさの 2 つの素数の積である 1024 ビット以上の整数の素因数分解の有する困難性に基づくものであることとする。

技術的基準第 2 条　規則第 2 条の基準を満たす電子署名の方式は、RSA 方式（オブジェクト識別子 1 2 840 113549 1 1 5）であってモジュラスとなる合成数が 1024 ビットのものとする。

○　電子証明書の発行に当たって都道府県知事が行う電子署名の方式

法律第 3 条第 6 項　前項の規定による通知を受けた都道府県知事は、総務省令で定めるところにより、当該都道府県知事が電子署名を行った当該申請に係る電子証明書を発行し、これを住所地市町村長に通知するものとする。

施行規則第 10 条第 1 項　法第 3 条第 6 項の規定による電子証明書の発行は、都道府県知事の使用に係る電子計算機の操作によるものとし、電子証明書の発行の方法に関する技術的基準については、総務大臣が定める。

技術的基準第 8 条第 2 項　発行者署名符号を用いて行う電子署名の方式は、RSA 方式（オブジェクト識別子 1 2 840 113549 1 1 5）であってモジュラスとなる合成数が 2048 ビットのものとする。

○　特定認証業務を行う者に係る認定の基準

法第 17 条第 1 項　次に掲げる者は、利用者から通知された電子署名が行われた情報について当該利用者が当該電子署名を行ったことを確認するため、都道府県知事に対して次条第 1 項の規定による同項に規定する保存期間に係る失効情報の提供及び同条第 2 項の規定による同項に規定する保存期間に係る失効情報ファイルの提供を求めようとする場合（第 4 号及び第 5 号に掲げる者にあっては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場合に、第 6 号に掲げる団体にあっては行政手続等における情報通信の技術の利用に関する法律第 2 条第 2 号に規定する行政機関等（以下「行政機関等」という。）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場合に限る。）には、あらかじめ、当該都道府県知事に対し、総務省令で定めるところにより、これらの提供を求める旨の届出をしなければならない。

第 5 号　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

施行令第 8 条　法第 17 条第 1 項第 5 号の政令で定める基準は、特定認証業務（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）第 2 条第 3 項に規定する特定認証業務をいう。以下この条において同じ。）を行う者が行う特定認証業務が次の各号のいずれにも該当することとする。

第 3 号　前号に掲げるもののほか、特定認証業務が総務省令で定める基準に適合する方法により行われるものであること。

施行規則第 26 条　令第 8 条第 3 号の総務省令で定める基準は、次に掲げるとおりとする。

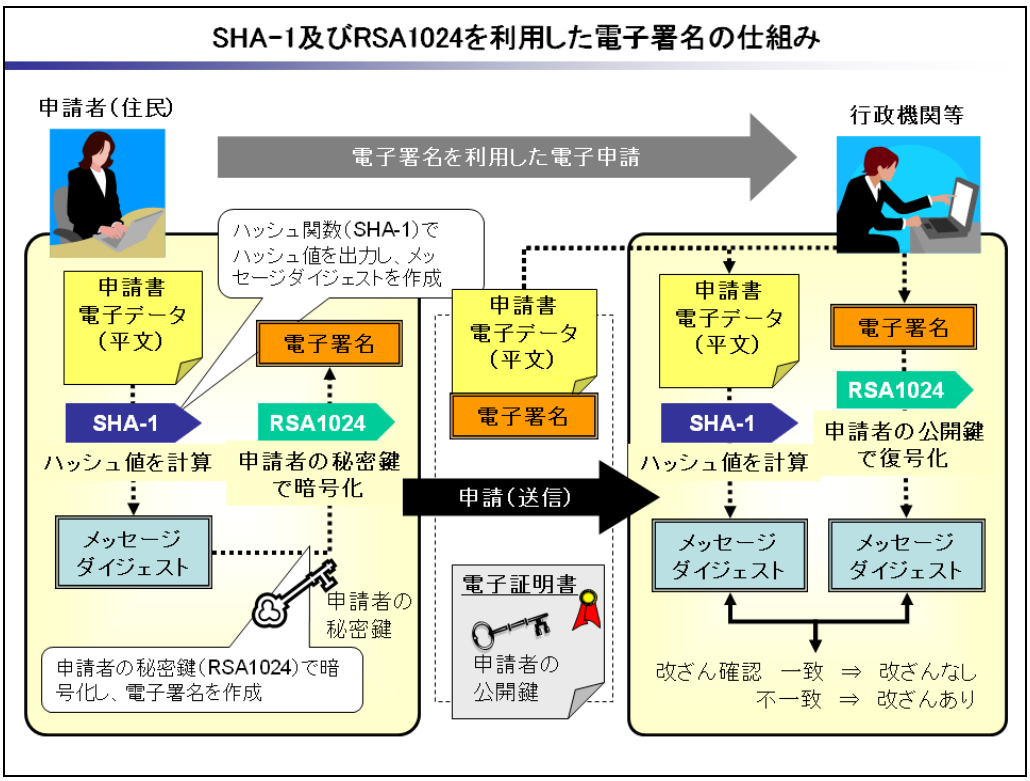
第 7 号　認証業務に関し、利用者その他の者が認定申請者が行う特定認証業務と他の業務を誤認することを防止するための適切な措置を講じていること。

技術的基準第 31 条　規則第 26 条第 7 号に規定する利用者その他の者が認定申請者が行う特定認証業務と他の業務を誤認することを防止するための適切な措置には、次の各号に掲げる措置が含まれるものとする。

第 2 号　発行者署名検証符号（電子署名及び認証業務に関する法律施行規則第 6 条第 9 号に規定する発行者署名検証符号をいう。次条において同じ。）

に係る電子証明書の値を SHA-1 で変換した値によって当該特定認証業務を特定すること。

図 2　SHA-1 及び RSA1024 を利用した電子署名の仕組み



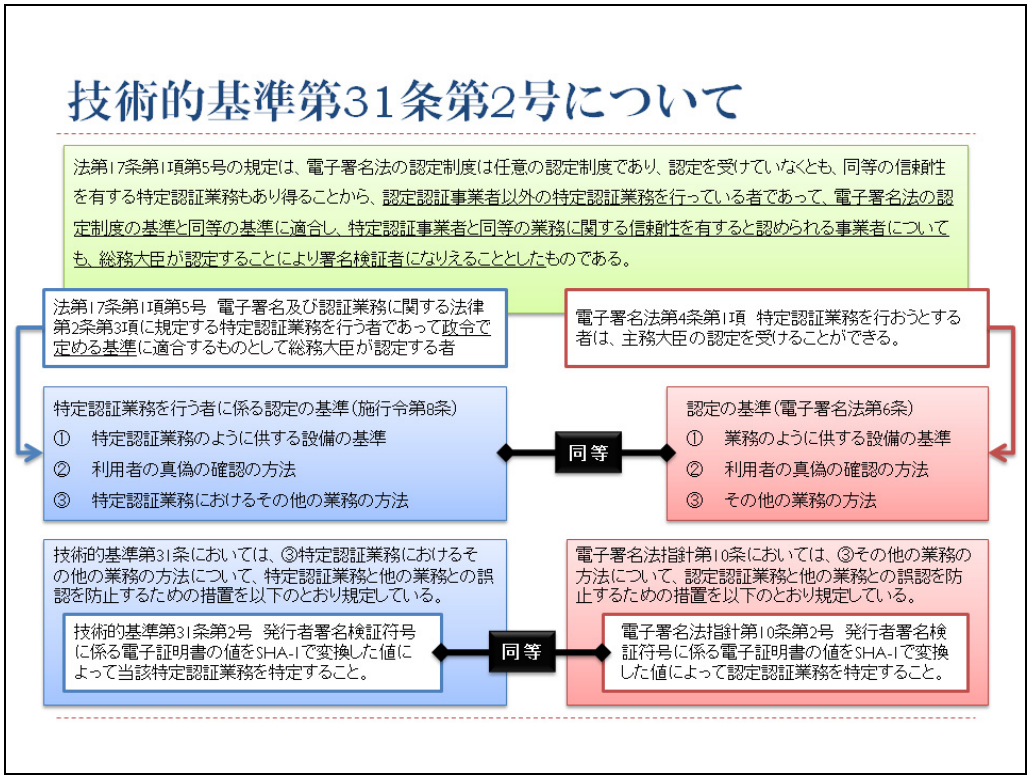
2.3.　本検討会の検討事項

本検討会においては、公的個人認証サービスにおいて利用する暗号アルゴリズムを規定する法令等のうち、暗号技術検討会等において安全性の低下により将来問題が生じる可能性が指摘されている SHA-1 及び RSA1024 の利用を規定する法令等について主に検討を行う。ただし、技術的基準第 31 条第 2 号の規定は、施行令第 8 条に規定する特定認証業務を行う者に係る認定の基準のうち、特定認証業務と他の業務との誤認を防止するための措置について、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 4 月 27 日総務省・法務省・経済産業省告示第 2 号。以下「電子署名法指針」という。）第 10 条第 2 号（*1）に規定する認定認証業務と他の業務との誤認を防止するための措置と同等の措置を定めるものであるため、技術的基準第 31 条第 2 号に規定する特定認証業務と他の業務との誤認を防止するための措置については、電子署名法指針第 10 条第 2 号に規定する措置に関する今後の改正を参考にすることとし、本検討会の検討事項には含めない（図 3 を参照のこ

と。)。このため、本検討会の主な検討事項は、施行規則第 2 条に規定する電子署名の基準、技術的基準第 2 条に規定する利用者等が行う電子署名の方式及び技術的基準第 8 条第 2 項に規定する電子証明書の発行に当たって都道府県知事が行う電子署名の方式とする。

*1
電子署名法指針第 10 条第 2 号　発行者署名検証符号に係る電子証明書の値を SHA-1 で変換した値によって認定認証業務を特定すること。

図 3　技術的基準第 31 条第 2 号について



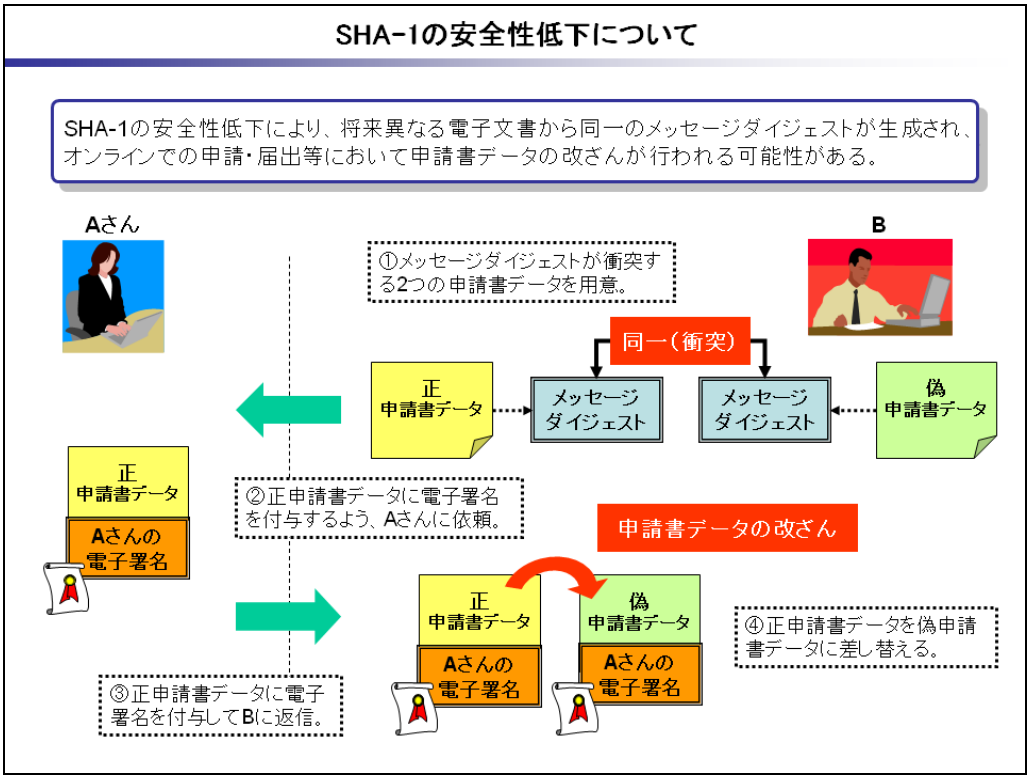
3. 公的個人認証サービスにおける暗号アルゴリズムの移行の必要性

3.1. SHA-1 及び RSA1024 の安全性評価

3.1.1. SHA-1 の安全性評価

SHA-1 の安全性低下により、将来異なる電子文書から同一のメッセージダイジェストが生成され、オンラインでの申請・届出等において申請書データの改ざんが行われる可能性がある。

図 4　SHA-1 の安全性低下について

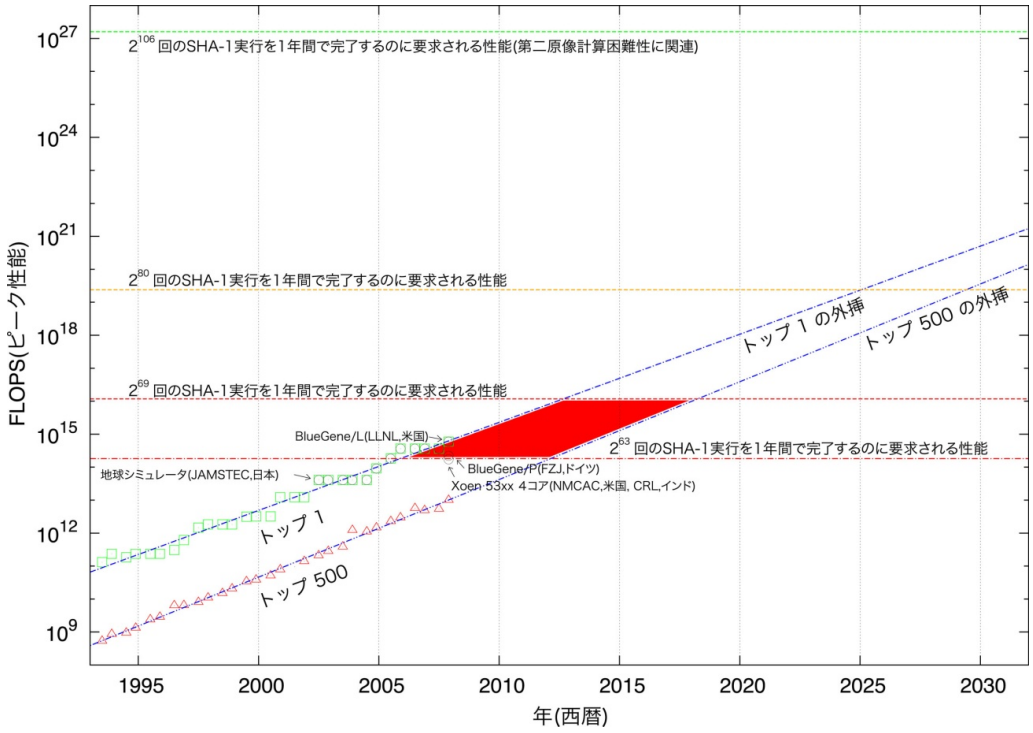


SHA-1 の安全性については、「SHA-1 の安全性に関する見解」（平成 18 年 6 月 28 日暗号技術監視委員会）において、「CRYPTREC[6]で検証した結果、2^{69} 回の SHA-1

[6] CRYPTREC とは Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。総務省及び経済産業省が共同で開催する暗号技術検討会（座長：今井秀樹中央大学教授）と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する暗号技術監視委員会（委員長：今井秀樹中央大学教授）及び暗号モジュール委員会（委員長：松本勉横浜国立大学教授）で構成される。（出典：CRYPTREC の Web サイト http://www.cryptrec.go.jp/about.html）

の実行回数で衝突発見できることの妥当性は検証された。また、近い将来に 2^{63} 回以下の SHA-1 の実行回数で衝突発見できることも妥当性があるとの結論を得た」と指摘され、「電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規（更新を含む）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、SHA-256 ビット以上のハッシュ関数の使用」が薦められている。また、電子署名法の施行状況に係る検討会報告書において、「衝突計算攻撃による脅威[7]は、2015 年前後には現実的になることが想定されるので、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」と評価されている。

図 5　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[8]



3.1.2.　RSA1024 の安全性評価

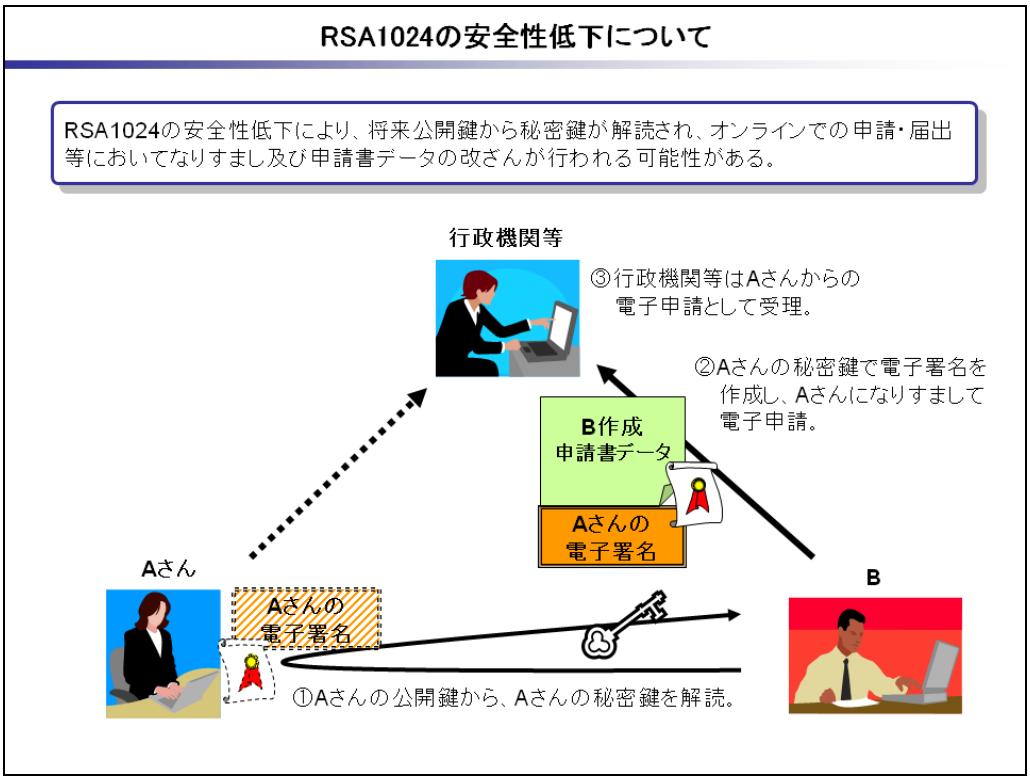
RSA1024 の安全性低下により、将来公開鍵から秘密鍵が解読され、オンラインでの申請・届出等においてなりすまし及び申請書データの改ざんが行われる可能性がある。

---

[7] 電子署名がない複数の異なる電子文書に同一の電子署名が付される脅威。（出典：電子署名法の施行状況に係る検討会報告書 13 頁）

[8] 出典：電子署名法の施行状況に係る検討会報告書 15 頁

図 6　RSA1024 の安全性低下について



RSA1024 の安全性については、「暗号技術検討会 2006 年度報告書」（2007 年 3 月）において、「新たな攻撃法によって、安全性に懸念を持たせるような事態は生じていないと判断した」が、「計算機性能の向上による計算能力の増大が主な危殆化[9]の要因とした場合[10]、攻撃者の獲得可能な解読計算能力が、HPC[11]の傾向を最もよく示すという意味で、スーパーコンピュータの世界第 1 位[12]と同等なレベルで向上していくと仮定すると、法パラメータ n=pq のサイズが 1024 ビットの IFP （n=pq 型素因数分解問題）が 1 年間の計算によって攻撃可能になる時期については、2010 年～2020 年の間と推定することができた」と指摘されている。また、電子署名法の施行状況に係る検討会報告書において、RSA1024 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が示されている」と評価されている。

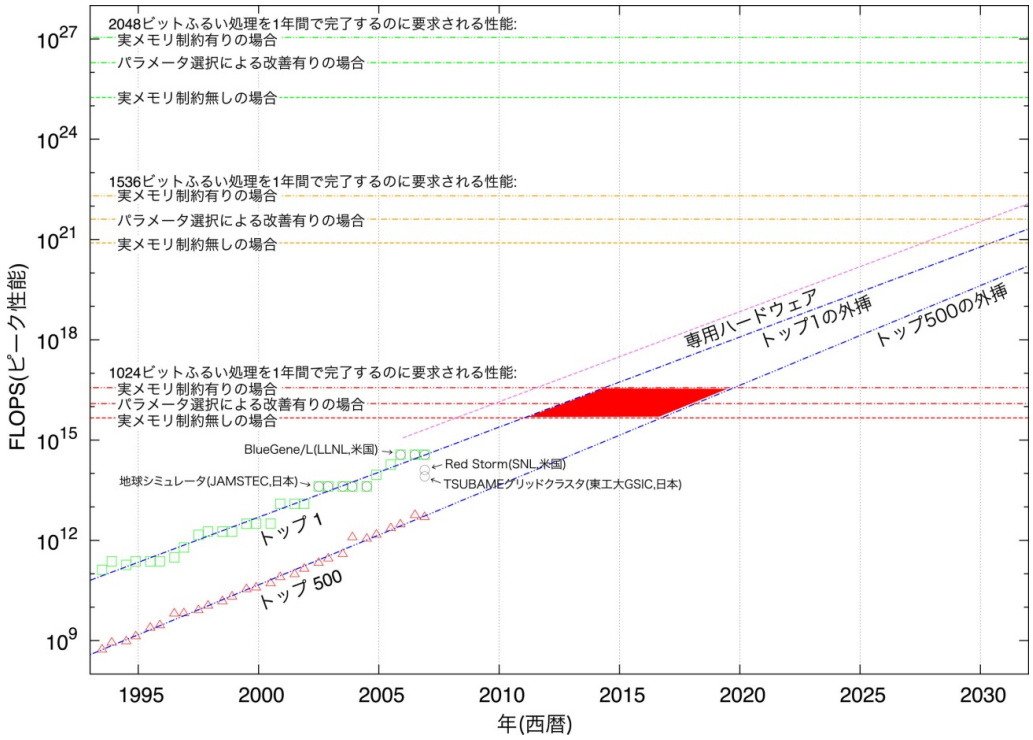
9 危うくなること。

10 今後の研究によって、一般数体ふるい法等のアルゴリズムの改良により処理時間が短縮することがあり得る。（出典：「暗号技術検討会 2006 年度報告書」13 頁）

11 High Performance Computing の略。（出典：「暗号技術検討会 2006 年度報告書」13 頁）

12 TOP500.Org の Web サイト、http://www.top500.org/による。（出典：「暗号技術検討会 2006 年度報告書」13 頁）

図 7　1 年間でふるい処理を完了するのに要求される処理性能の予測[13] [14]



3.2.　政府機関における暗号アルゴリズムの安全性低下への対応

政府機関における暗号アルゴリズムの安全性低下への対応については、情報セキュリティ政策会議において移行指針が決定された。移行指針の内容のうち、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に関連する主なものは以下のとおりである。

- SHA-1 及び RSA1024 は、電子申請、電子入札等を行うための政府機関の情報システムにおいて、その安全性及び信頼性を確保するための技術の一要素として広く使用されている暗号アルゴリズムである。政府機関の情報システムの安全性及び信頼性を確保するためには、これらの暗号アルゴリズムについて、情報システムのライフサイクル等を踏まえつつ、適時により安全なものに移行する必要がある。

[13] 出典：「CRYPTREC Report 2006」（平成 19 年 3 月）17 頁

[14] 参考（コスト）：地球シミュレータ（海洋研究開発機構）約 400 億円、TSUBAME（東京工業大学)約 20 億円、BlueGene/L（米国ローレンス・リバモア国立研究所）約 1 億ドル、Red Storm（米国サンディア国立研究所）約 9000 万ドル（出典：「暗号技術検討会 2006 年度報告書」12 頁）

- 政府認証基盤（GPKI）及び商業登記認証局並びに政府認証基盤に依存する情報システムについて、SHA-1 及び RSA1024 に代わる暗号アルゴリズムとして SHA-256 及び RSA2048 を使用する。

- 内閣官房、総務省、法務省、経済産業省等は、新たな暗号アルゴリズムへの切替時期並びに SHA-1 及び RSA1024 の使用停止時期について、2008 年度中に検討する。

- 内閣官房、総務省等は、政府認証基盤と他の認証局との相互接続に必要となる技術要件及び新たな暗号アルゴリズムへの移行が完了する以前に安全性の低下による影響が発生する状況に備えた官民共同の電子証明書の失効等の仕組みについて、2008 年度当初に検討に着手する。

- 各府省庁は、2010 年度から 2013 年度までの間に各情報システムの対応を完了する。

- 総務省及び経済産業省は、現在使用されている SHA-1 及び RSA1024 並びに新たに使用する SHA-256 及び RSA2048 の安全性について監視し、内閣官房は、必要な情報を速やかに各府省庁に提供する。

3.3. 電子署名法に関する暗号アルゴリズムの移行

電子署名法に関する暗号アルゴリズムの移行については、電子署名法の施行状況に係る検討会において電子署名法の施行状況に係る検討会報告書が取りまとめられた。電子署名法の施行状況に係る検討会報告書の内容のうち、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に関連する主なものは以下のとおりである。

- 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[15]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。

[15] 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。（出典：電子署名法の施行状況に係る検討会報告書 13 頁）

- 電子署名法指針第 3 条（*2）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（SHA-256、SHA-384 及び SHA-512）を追加し、SHA-2 及び RSA2048 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。

*2

電子署名法指針第 3 条　規則第 2 条の基準を満たす電子署名の方式は、次の各号のいずれかとする。

第 1 号　RSA 方式（オブジェクト識別子 1 2 840 113549 1 1 5）又は RSA-PSS 方式（オブジェクト識別子 1 2 840 113549 1 1 10）であって、モジュラスとなる合成数が 1024 ビット以上のもの

電子署名及び認証業務に関する法律施行規則第 2 条　法第 2 条第 3 項の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。

第 1 号　ほぼ同じ大きさの二つの素数の積である 1024 ビット以上の整数の素因数分解

電子署名法第 2 条第 3 項　この法律において「特定認証業務」とは、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。

- 電子署名法では、電子署名法第 3 条（*3）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、特定認証業務に対する認定制度を設けている。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、その暗号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（*4）自体を満たさなくなるため、特定認証業務の要件として電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日総務省・法務省・経済産業省令第２号）第２条及び電子署名法指針第３条において SHA-1 及び RSA1024 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。

*3

電子署名法第3条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

*4

電子署名法第2条第1項　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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。

第1号　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。

第2号　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。

- 総務省、法務省及び経済産業省においては、表1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、RSA1024 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。今後総務省、法務省及び経済産業省は、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。

表 1　電子署名法に関する暗号アルゴリズムの移行スケジュール案

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) *移行指針による
(2013 年度)	(政府機関システム新旧暗号アルゴリズム対応環境構築が完了) *移行指針による
2014 年度早期まで	認定認証事業者は、RSA2048 による発行者鍵ペアを活性化させ SHA-2 及び RSA2048 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 及び RSA1024 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 及び RSA1024 を削除。(SHA-1 及び RSA1024 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 及び RSA2048 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。)

3.4.　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の必要性

暗号技術検討会等において SHA-1 及び RSA1024 の安全性低下により将来問題が生じる可能性が上記のとおり指摘されており、SHA-1 及び RSA1024 を利用した電子署名が、将来電子署名法第 3 条に規定する「真正な成立の推定」の効果を受けるための要件である「本人だけが行うことができる電子署名」又は電子署名法第 2 条第 1 項に規定する電子署名の要件自体に該当しなくなる可能性がある。このため、公的個人認証サービスの安全性及び信頼性を引き続き確保するためには、公的個人認証サービスにおいて利用されている SHA-1 及び RSA1024 について、より安全な暗号アルゴリズムに移行する必要がある。また、政府機関における暗号アルゴリズムの安全性低下への対応及び電子署名法に関する暗号アルゴリズムの移行については上記のとおりであることから、公的個人認証サービスの情報システムと政府機関の情報システム及び電子署名法に規定する特定認証業務に係る情報システムの相互運用性を確保する観点からも、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が必要である。

4. 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案

4.1. SHA-1 及び RSA1024 に代わる暗号アルゴリズム

SHA-1 及び RSA1024 に代わる暗号アルゴリズムに関して、政府認証基盤（GPKI）及び商業登記認証局並びに政府認証基盤に依存する情報システムについては移行指針において SHA-256 及び RSA2048 が示されており、特定認証業務に係る電子署名の基準については電子署名法の施行状況に係る検討会報告書において SHA-2（SHA-256、SHA-384 及び SHA-512）及び RSA2048 が示されている。このため、公的個人認証サービスにおいては、SHA-1 及び RSA1024 に代わる暗号アルゴリズムとして SHA-256 及び RSA2048 を利用することが適当である。また、電子証明書の発行に当たって都道府県知事が行う電子署名に利用する暗号アルゴリズムのうち、RSA2048 については引き続き利用することが適当である。

なお、SHA-256 の安全性については、「暗号技術検討会 2005 年度報告書」（2006 年 3 月）において「実用的な安全性を脅かす攻撃方法が報告されていないため、」「応用分野で使うのに十分安全であると考えられる」と評価されている（RSA2048 の安全性については図 7 を参照のこと。）。

4.2. 暗号アルゴリズムの移行スケジュール

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に当たっては、SHA-256 及び RSA2048 に対応する公的個人認証サービスセンターシステムの構築、鍵ペア生成装置及び受付窓口端末の調達、公的個人認証サービスアプリケーションの開発、住民基本台帳カード（以下「住基カード」という。）の交付等が必要となるため、暗号アルゴリズムの円滑な移行に向けて、移行スケジュールは予め示されることが望ましい。移行スケジュールについて、具体的には SHA-256 及び RSA2048 による電子証明書（以下「新電子証明書」という。）の発行開始時期（SHA-256 及び RSA2048 による電子署名に係る認証業務の開始時期。移行指針中の「新たな暗号アルゴリズムへの切替時期」に対応するもの。）、SHA-1 及び RSA1024 による電子証明書（以下「旧電子証明書」という。）の発行停止時期、SHA-1 及び RSA1024 による電子署名に係る認証業務の停止時期（移行指針中の「SHA-1 及び RSA1024 の使用停止時期」に対応するもの。以下「SHA-1 及び RSA1024 の使用停止時期」という。）を検討する必要がある。

まず、新電子証明書の発行開始時期については、以下の事項を考慮すると 2014 年

度早期とすることが適当である。また、旧電子証明書の発行停止時期については、新電子証明書及び旧電子証明書を併行して発行することとなった場合、公的個人認証サービスセンターシステムの運用費用及び鍵ペア生成装置の調達費用が増大すると考えられるため、新電子証明書の発行開始時期と同時期（2014 年度早期）とすることが適当である。

- 電子署名法の施行状況に係る検討会報告書において、SHA-1 の安全性については「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」、また RSA1024 の安全性については「概ね 2015 年以降に、危殆化のおそれが高まってくることが示されている」と指摘されている。

- 政府機関における暗号アルゴリズムの安全性低下への対応について、各府省庁は 2010 年度から 2013 年度までの間に各情報システムの対応を完了することが、移行指針において示されている。

- 電子署名法に関する暗号アルゴリズムの移行については、電子署名法の施行状況に係る検討会報告書において SHA-2 及び RSA2048 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」と指摘されている。

- 2011 年度末を目途に新たな暗号アルゴリズムに対応する住基カードの交付を開始することが検討されている。

次に、SHA-1 及び RSA1024 の使用停止時期については、以下の事項を考慮すると、現段階では上記の旧電子証明書の発行停止時期（2014 年度早期）及び電子証明書の有効期間（3 年）を踏まえた時期（2017 年度早期。ただし、電子証明書の有効期間は今後延長される可能性があり、有効期間が 5 年に延長された場合には 2019 年度早期）とすることが適当である。

- RSA1024 の安全性について、「暗号技術検討会 2006 年度報告書」において「1 年間の計算によって攻撃可能になる時期については、2010 年～2020 年の間と推定することができた」と指摘されている。

- 現在、電子証明書は住基カードに記録されており、SHA-1 及び RSA1024 の使用停止時期を 2015 年度早期又は 2016 年度早期とした場合、電子証明書の有効期間（3 年）中に電子証明書が失効するとともに、住基カードの有効期間（10 年）

中に住基カードが失効するため、利用者の利便性を損なう。また、特定の時期（SHA-1 及び RSA1024 の使用停止時期直後等）に多くの利用者が市町村の窓口で電子証明書及び住基カードの再発行を申請することになるため、公的個人認証サービスの運営及び市町村における住基カードの発行業務に混乱が生じるおそれがある。

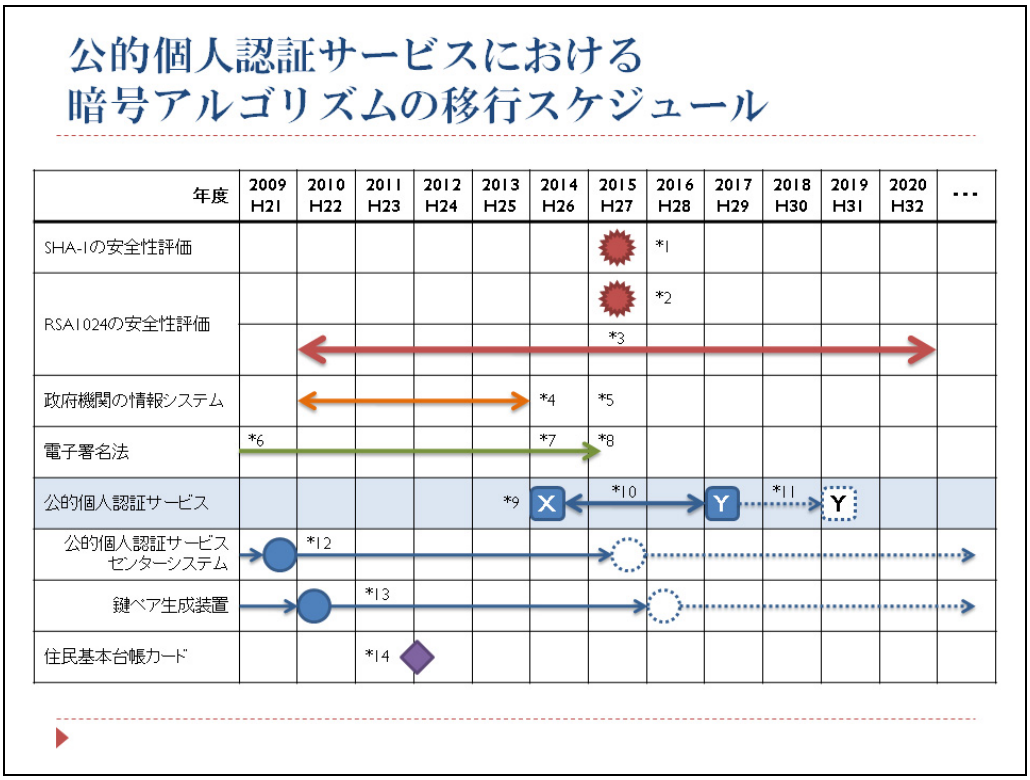
このため、総務省において、現段階では表 2 のスケジュールを基本として施行規則第 2 条並びに技術的基準第 2 条及び第 8 条第 2 項の改正作業等を進めていくことが適当である。ただし、このスケジュールについては SHA-1 及び RSA1024 の急速な安全性低下を前提としていないため、今後、SHA-1 及び RSA1024 の使用停止時期以前に SHA-1 及び RSA1024 の安全性低下により問題が生じる状況に備え、暗号技術検討会等の意見等を踏まえコンティンジェンシープラン[16]を検討する必要がある。また、利用者の利便性及び「5. 今後の検討事項」に十分配慮して公的個人認証サービスにおける暗号アルゴリズムの移行を進める必要がある。

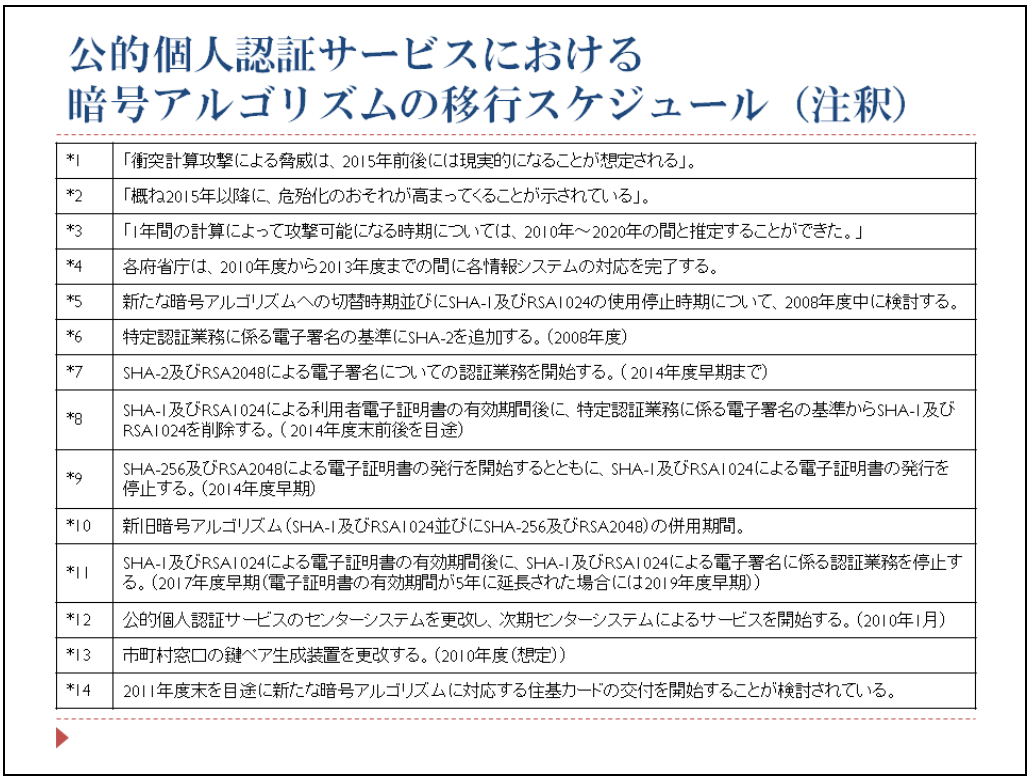
表 2　公的個人認証サービスにおける暗号アルゴリズムの移行スケジュール

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。
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。

16 不測の事態に対する対処法を予め定めた計画。

図８　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





4.3. 暗号アルゴリズムの移行案の見直し

上記の暗号アルゴリズムの移行案については、暗号技術検討会等における暗号アルゴリズムの監視状況、政府機関における暗号アルゴリズムの安全性低下への対応状況、電子署名法に関する暗号アルゴリズムの移行状況、公的個人認証制度の改正状況等を踏まえ、必要に応じて見直しを行う必要がある。

5. 今後の検討事項

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を円滑に進めるため、以下の事項について今後検討を行う必要がある。

- SHA-1 及び RSA1024 の使用停止時期以前に SHA-1 及び RSA1024 の安全性低下により問題が生じる状況に備え、暗号技術検討会等の意見等を踏まえコンティンジェンシープランを検討する必要がある。

- SHA-256 及び RSA2048 に対応する公的個人認証サービスセンターシステムの構築、鍵ペア生成装置及び受付窓口端末の調達、公的個人認証サービスアプリケーションの開発、住基カードの交付等について、手順、スケジュール、所要の経費等を検討する必要がある。

- 電子署名を行う電子文書のうち、長期間にわたり利用するものについて対策を検討する必要がある。また、暗号アルゴリズムの移行に当たってセキュリティホールを作らないよう、暗号アルゴリズムの安全な移行方法を検討する必要がある。

参考資料

参考資料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
開催要領

1. 目的

公的個人認証サービスにおいて利用されているハッシュ関数 SHA-1 及び公開鍵暗号方式 RSA1024 の安全性に懸念が生じる可能性が指摘され、国際的にも新たな暗号方式等への移行が進んでいることから、公的個人認証サービスの信頼性を引き続き確保するため、暗号方式等の移行について学識経験者・関係機関等による検討を行う。

2. 検討事項

- 公的個人認証サービスにおける暗号方式等の移行方針について

3. 構成及び運営

- 検討会の構成は別紙のとおりとする。
- 検討会には座長１名を置く。
- 会議資料及び議事要旨は、総務省ホームページに掲載することにより公表する。

4. 開催期間

平成 20 年 9 月から平成 20 年 12 月まで計 3 回の開催を予定。

5. 事務局

総務省自治行政局地域政策課地域情報政策室が検討会の庶務を担当する。

別紙

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
構成員・オブザーバー名簿

構成員

井　堀　幹　夫	市川市ＣＩＯ情報政策監
大　山　永　昭	東京工業大学像情報工学研究施設教授
小笠原　　章	徳島県県民環境部地域振興局地域情報政策課長
亀　田　　繁	財団法人日本情報処理開発協会電子署名・認証センター長
佐々木　良　一	東京電機大学未来科学部情報メディア学科教授
鈴　木　　豊	東京都総務局行政部副参事（振興調整担当）
竹　内　雅　彦	財団法人自治体衛星通信機構公的個人認証サービスセンター長
辻　井　重　男	情報セキュリティ大学院大学学長　【座長】
山　戸　康　弘	大分県企画振興部ＩＴ推進課長

オブザーバー

相　澤　　哲	法務省民事局商事課長
新　井　孝　雄	総務省情報流通行政局情報流通振興課情報セキュリティ対策室長
伊　藤　毅　志	内閣官房情報セキュリティセンター内閣参事官
岡　本　好　史	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室長
古　賀　　明	国税庁長官官房企画課情報技術室長
田　中　　宏	総務省情報通信国際戦略局通信規格課長
丸　山　淑　夫	総務省自治行政局市町村課長
三　角　育　生	経済産業省商務情報政策局情報セキュリティ政策室長

（敬称略・五十音順）

参考資料 2

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
開催状況

開催時期	議事
第 1 回 平成 20 年 9 月 16 日	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の開催について ②　SHA-1 及び RSA1024 の安全性評価について ③　政府機関における暗号の安全性低下への対応について ④　「電子署名及び認証業務に関する法律」に関する暗号アルゴリズムの移行について ⑤　住民基本台帳カードの対応について
第 2 回 平成 20 年 10 月 28 日	①　政府認証基盤（GPKI）における暗号方式等の移行について ②　公的個人認証サービスにおけるシステム更改の状況と暗号アルゴリズムの移行に係る影響について ③　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案について ④　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案について
第 3 回 平成 20 年 12 月 18 日	①　検討会報告書案について ②　暗号移行のための残された検討課題について ③　公的個人認証サービスに関するリスク整理について

用語集

用語	解説
暗号アルゴリズム	情報を暗号化する手順。
危殆化	危うくなること。
CRYPTREC	電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。総務省及び経済産業省が共同で開催する暗号技術検討会（座長：今井秀樹中央大学教授）と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する暗号技術監視委員会（委員長：今井秀樹中央大学教授）及び暗号モジュール委員会（委員長：松本勉横浜国立大学教授）で構成される。（出典：CRYPTREC の Web サイト）
公開鍵暗号方式	関連した 2 つの鍵（公開鍵と秘密鍵）を使用する暗号方式であり、一方の鍵（公開鍵又は秘密鍵）で暗号化したデータは他方の鍵（秘密鍵又は公開鍵）でのみ復号できるようになっている。2 つの鍵は、公開鍵が与えられても、秘密鍵を導き出すことが計算上困難な特性を持っている。（出典：移行指針 1 頁）
コンティンジェンシープラン	不測の事態に対する対処法を予め定めた計画。
衝突計算攻撃による脅威	電子署名がない複数の異なる電子文書に同一の電子署名が付される脅威（出典：電子署名法の施行状況に係る検討会報告書 13 頁）
第二原像計算攻撃による脅威	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（出典：電子署名法の施行状況に係る検討会報告書 13 頁）
ハッシュ関数	与えられたデータから固定ビット長の値を生成する関数。（出典：移行指針 1 頁）