

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

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¹SHA-1 及び公開鍵暗号方式²RSA1024 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（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●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。

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私的検討会として開催。

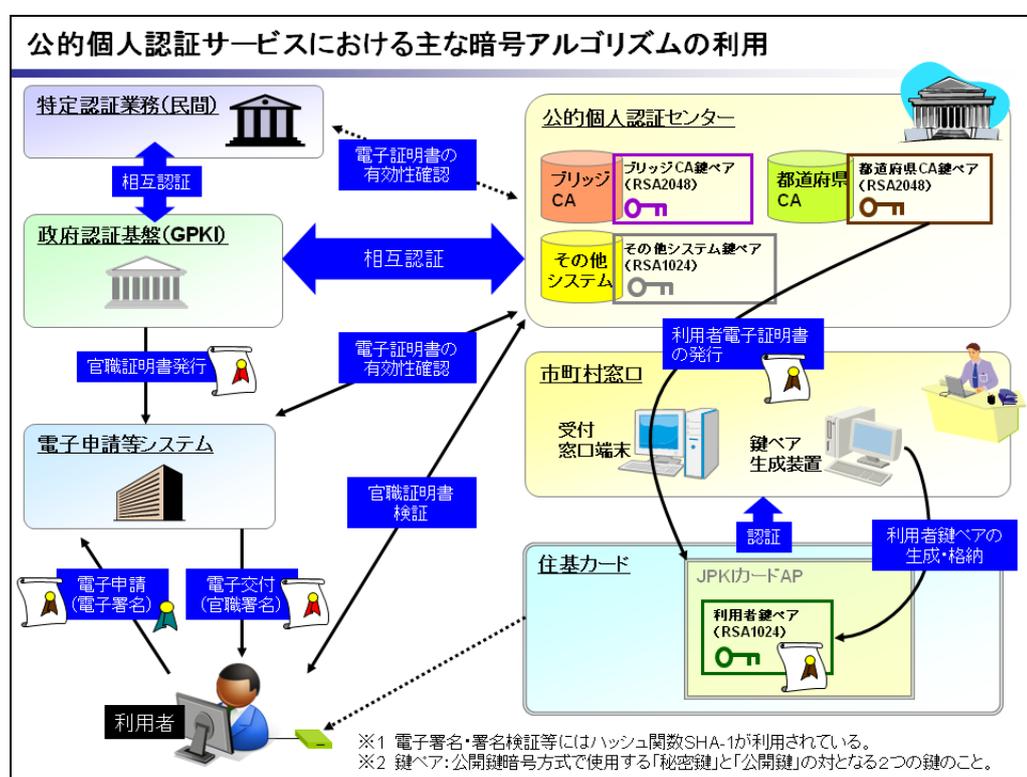
⁵ 情報を暗号化する手順。

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している法令等

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「政令」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「省

令」という。)及び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定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。

省令第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12840113549115)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。

省令第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12840113549115)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。

○ 特定認定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 号に掲げる者にあつ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つ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つ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

政令第 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。

省令第 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。

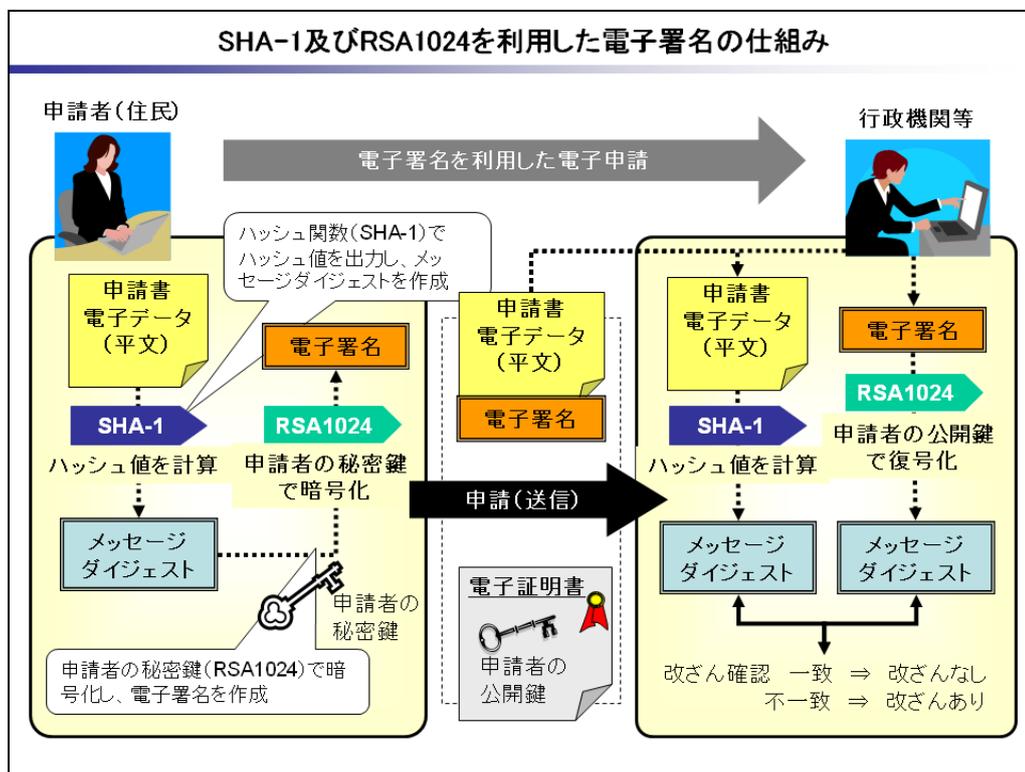
第 7 号 認証業務に関し、利用者その他の者が認定申請者が行う特定認証業務と他の業務を誤認することを防止するための適切な措置を講じていること。

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

本検討会の主な検討事項は、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している法令等のうち、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 の利用を規定している法令等とする。ただし、技術的基準第 31 条第 2 号の規定は、省令第 26 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事とし、本検討会の検討事項には含めない。このため、本検討会において

は、主に省令第 2 条に規定する電子証明書の基準、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について検討を行う。

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。

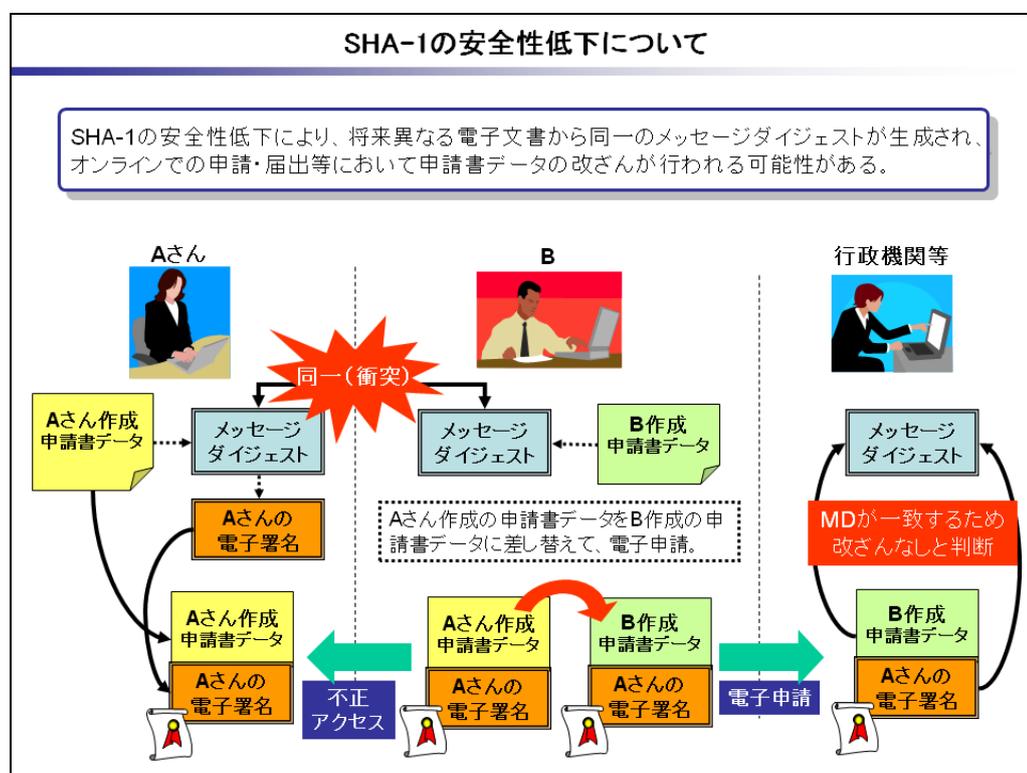
3. 公的個人認証サービスにおける暗号アルゴリズムの移行の必要性

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3 SHA-1 の安全性低下について

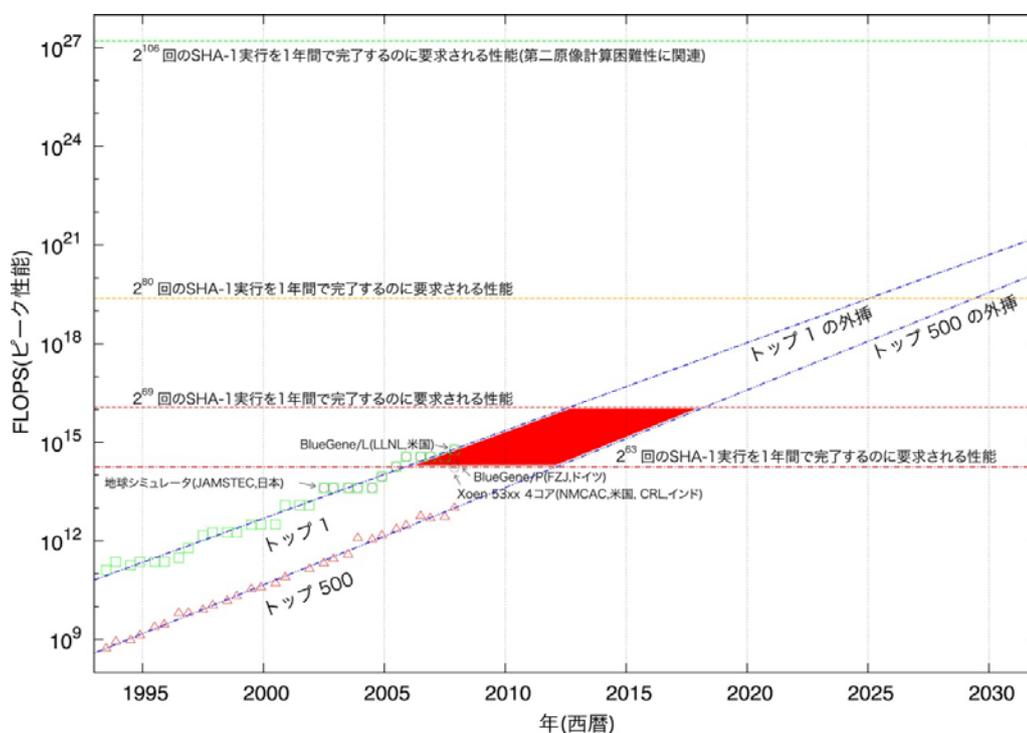


SHA-1 の安全性については、「SHA-1 の安全性に関する見解」（平成 18 年 6 月 28 日暗号技術監視委員会）において、「CRYPTREC⁶で検証した結果、2⁶⁹ 回の SHA-1

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 4 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⁾



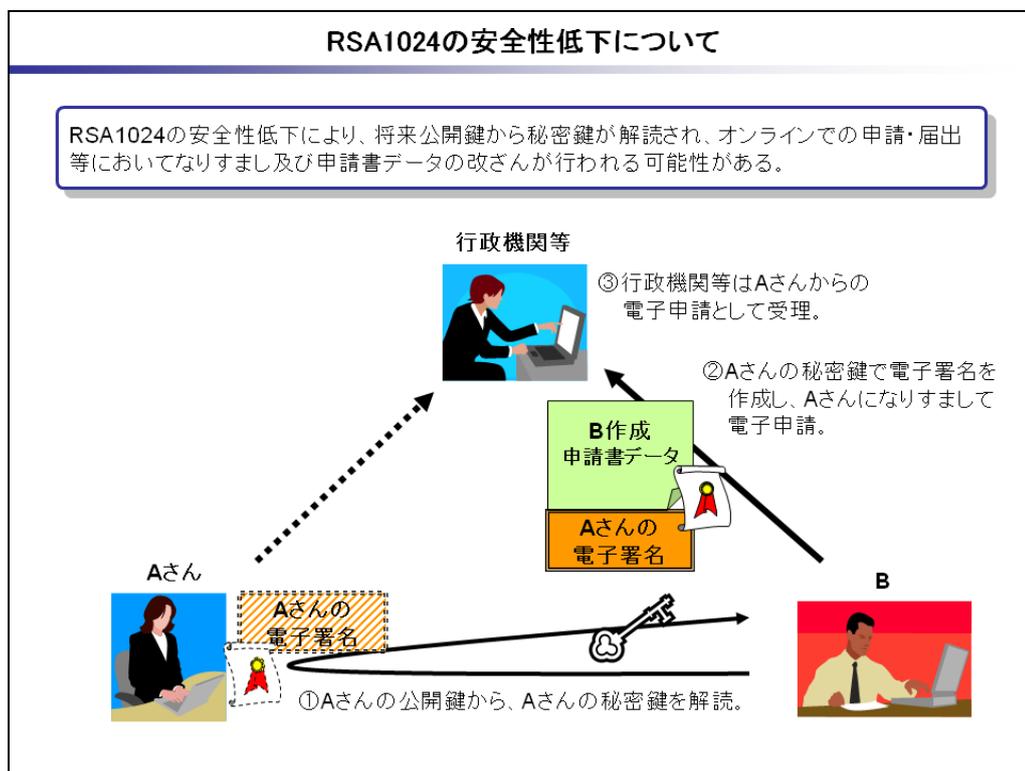
3.1.2. RSA1024 の安全性評価

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 5 RSA1024 の安全性低下について



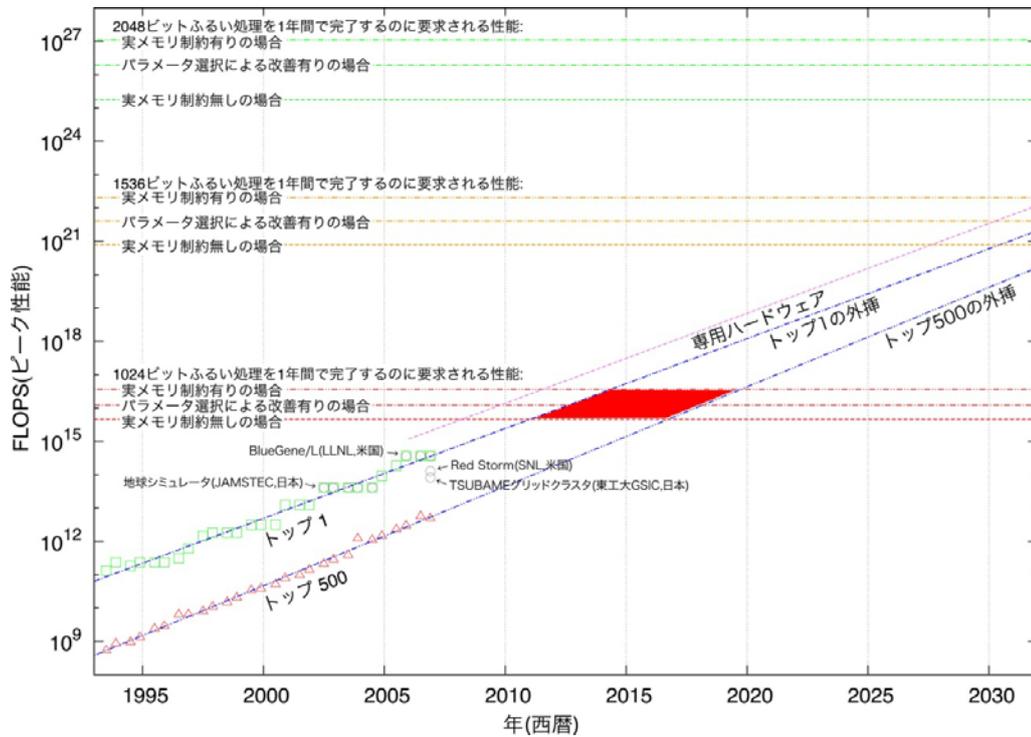
RSA1024 の安全性については、「暗号技術検討会 2006 年度報告書」（2007 年 3 月）において、「新たな攻撃法によって、安全性に懸念を持たせるような事態は生じていないと判断した」が、「計算機性能の向上による計算能力の増大が主な危殆化の要因とした場合⁹、攻撃者の獲得可能な解読計算能力が、HPC¹⁰の傾向を最もよく示すという意味で、スーパーコンピュータの世界第 1 位¹¹と同等なレベルで向上していくと仮定すると、法パラメータ $n=pq$ のサイズが 1024 ビットの IFP（ $n=pq$ 型素因数分解問題）が 1 年間の計算によって攻撃可能になる時期については、2010 年～2020 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を示されている」と評価されている。

⁹ 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が、今回の評価では無視している。（出典：「暗号技術検討会 2006 年度報告書」13 頁）

¹⁰ High Performance Computing の略。（出典：「暗号技術検討会 2006 年度報告書」13 頁）

¹¹ 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6 1年間でふり処理を完了するのに要求される処理性能の予測^{12 13}



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について

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。

¹² 出典：「CRYPTREC Report 2006」（平成 19 年 3 月）17 頁

¹³ 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、新たな暗号アルゴリズムとして SHA-256 及び RSA2048 を採用する。
- 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について

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。

- 電子署名法指針第 3 条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。

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。

電子署名及び認証業務に関する法律施行規則（以下「電子署名法施行規則」という。）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

- 電子署名法では、電子署名法第 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法施行規則第 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。

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。

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。

- 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。また、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 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、 <u>特定認証業務に係る電子署名の基準にSHA-2を追加。</u>
(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 <u>SHA-2及びRSA2048による電子署名についての認証業務を開始。</u>
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、 <u>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。</u> (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ついて、移行指針においては SHA-256 及び RSA2048 が示されており、電子署名法の施行状況に係る検討会報告書においては 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 を採用することが適当であり、省令第 2 条並びに技術的基準第 2 条及び第 8 条第 2 項の改正案は以下のとおりである。

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 6 を参照のこと。）。

○ 省令第 2 条並びに技術的基準第 2 条及び第 8 条第 2 項の改正案

省令第 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二つの素数の積である 2048 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 11） であってモジュラスとなる合成数が 2048 ビット以上のものとする。

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 11） 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。

以下の項目については、今後本検討会において議論する。

4.2. 暗号アルゴリズムの移行スケジュール

4.3. 新たに採用する暗号アルゴリズム及び移行スケジュールの見直し

5. 今後の検討事項