資料4

検討会報告書案について

総務省 地域力創造グループ 地域情報政策室

報告書骨子案

1. はじめに

① 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。

② 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SHA-1及び公開鍵暗号方式RSA1024について、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。

③ 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において、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等について報告書が取りまとめられ、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が決定された。

④ 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、計3回開催。

⑤ 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。

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（その１）

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。

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（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施行令（政令）、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規則（省令）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（技術的基準）に以下の内容を規定。

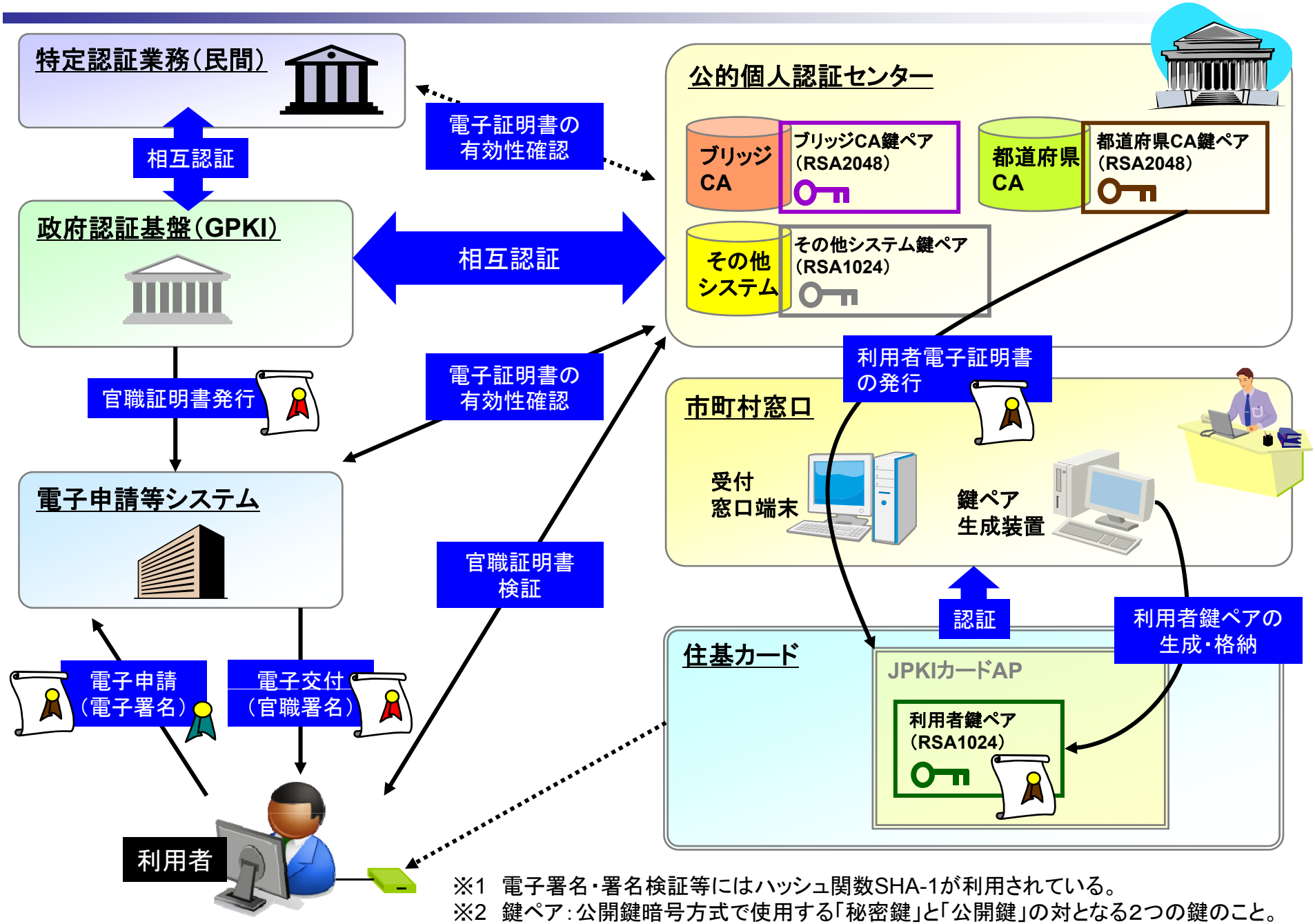
① 電子署名の基準及び利用者等が行う電子署名の方式

② 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

③ 特定認定業務を行う者に係る認定の基準

参考資料

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



※1　電子署名・署名検証等にはハッシュ関数SHA-1が利用されている。
※2　鍵ペア：公開鍵暗号方式で使用する「秘密鍵」と「公開鍵」の対となる2つの鍵のこと。

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（その２）

2.3. 本検討会の検討事項

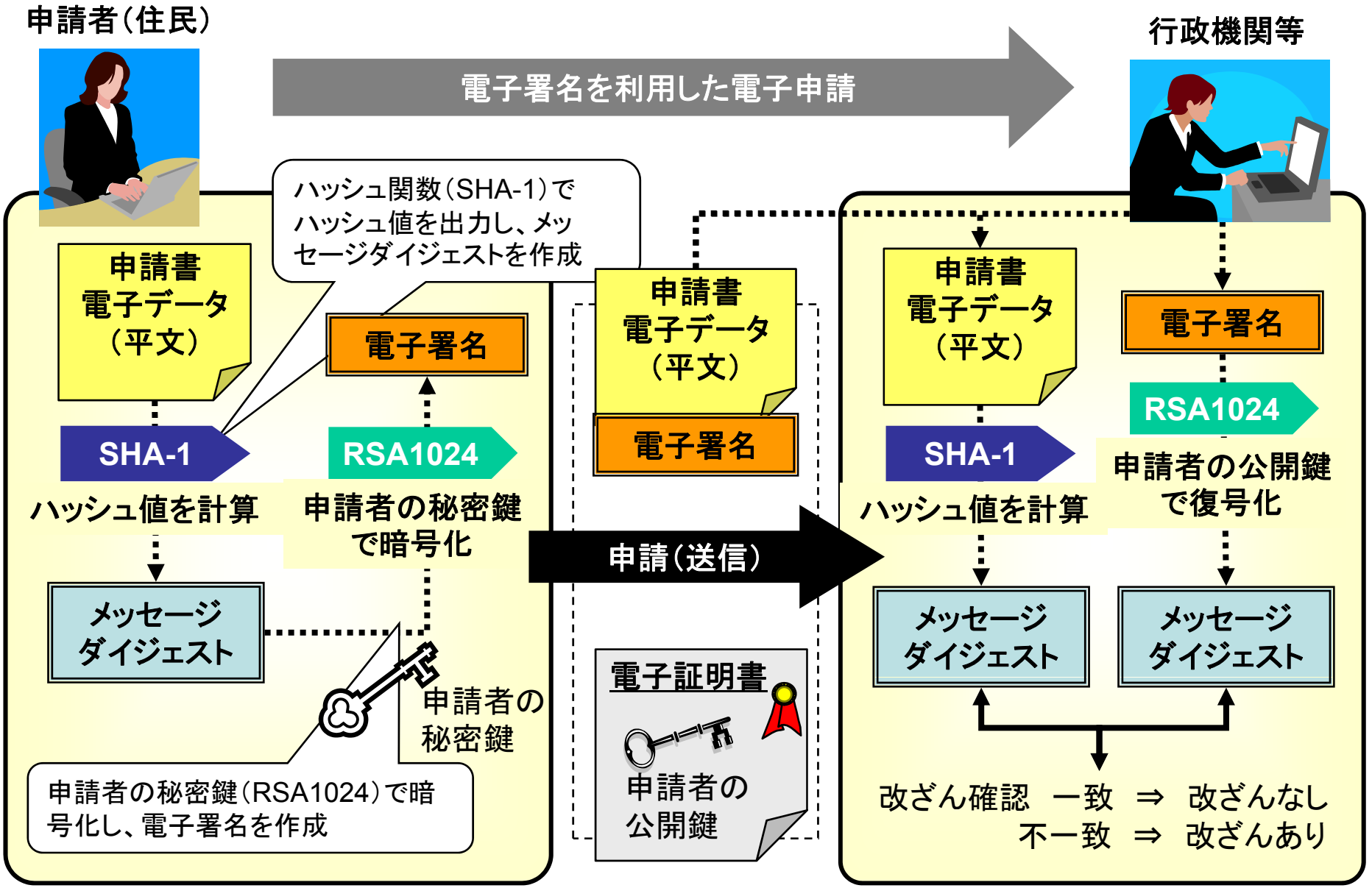
本検討会の主な検討事項は、公的個人認証サービスにおいて利用する暗号アルゴリズムを規定している法令等のうち、暗号技術検討会等において安全性の低下により将来問題が生じる可能性が指摘されているSHA-1及びRSA1024の利用を規定している法令等とする。ただし、技術的基準第31条第2号に規定する特定認証業務と他の業務との誤認を防止するための措置については、電子署名法指針第10条第2号に規定する措置に関する今後の改正を参考にすることとし、本検討会の検討事項には含めない。このため、本検討会においては、主に以下の事項について検討を行う。

① 省令第2条に規定する電子証明書の基準
② 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
③ 技術的基準第8条第2項に規定する都道府県知事が行う電子署名の方式

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 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。
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。

参考資料

SHA-1及びRSA1024を利用した電子署名の仕組み



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（その１）

SHA-1の安全性評価

● 「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）

「CRYPTRECで検証した結果、2^{69}回のSHA-1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。」

「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を薦める。」

● 電子署名法の施行状況に係る検討会報告書

「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」

RSA1024の安全性評価

● 「暗号技術検討会2006年度報告書」
（2007年3月）

「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 、攻撃者の獲得可能な解読計算能力が、HPC 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 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。」

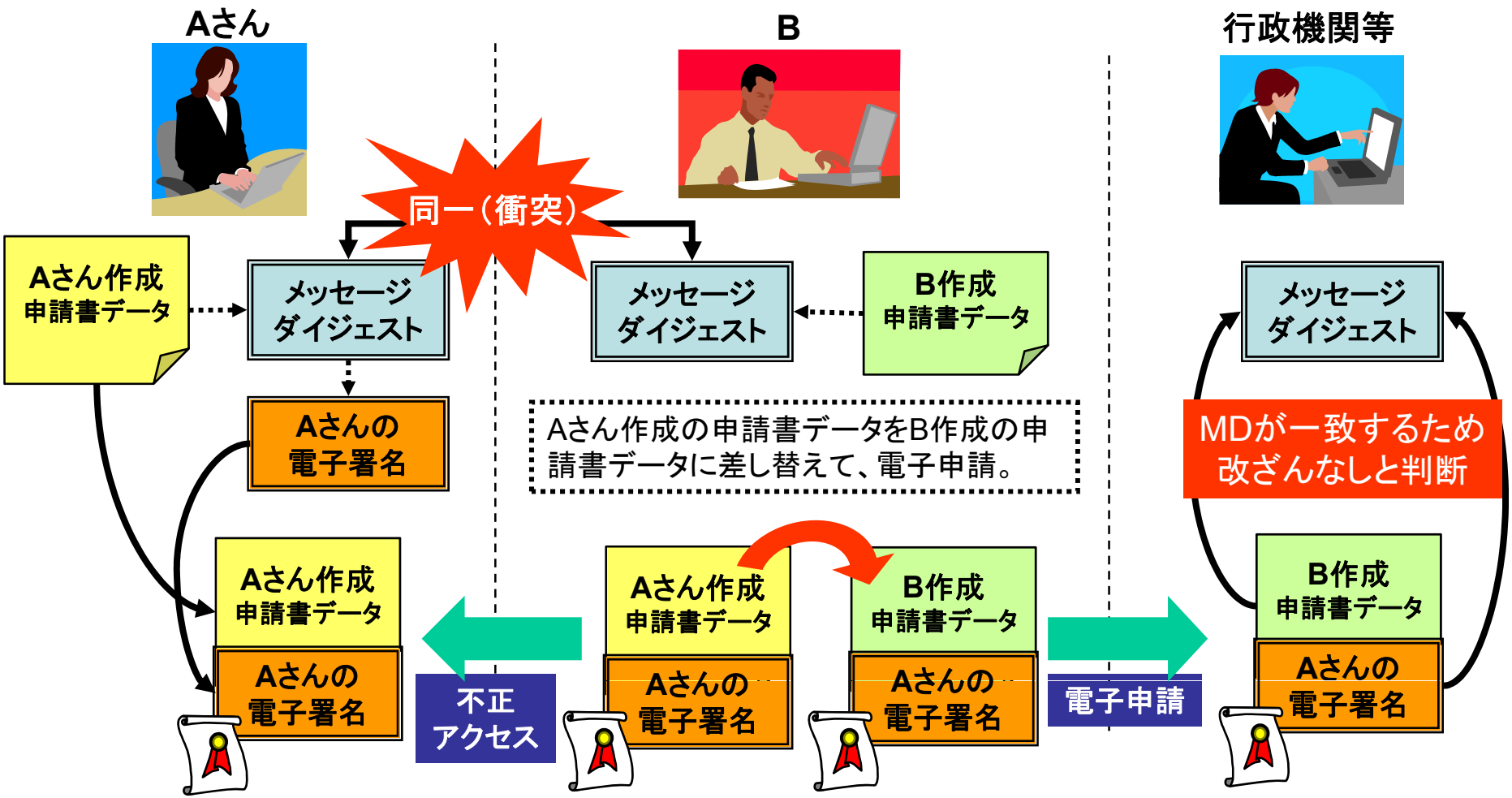
● 電子署名法の施行状況に係る検討会報告書

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」

参考資料

SHA-1の安全性低下について

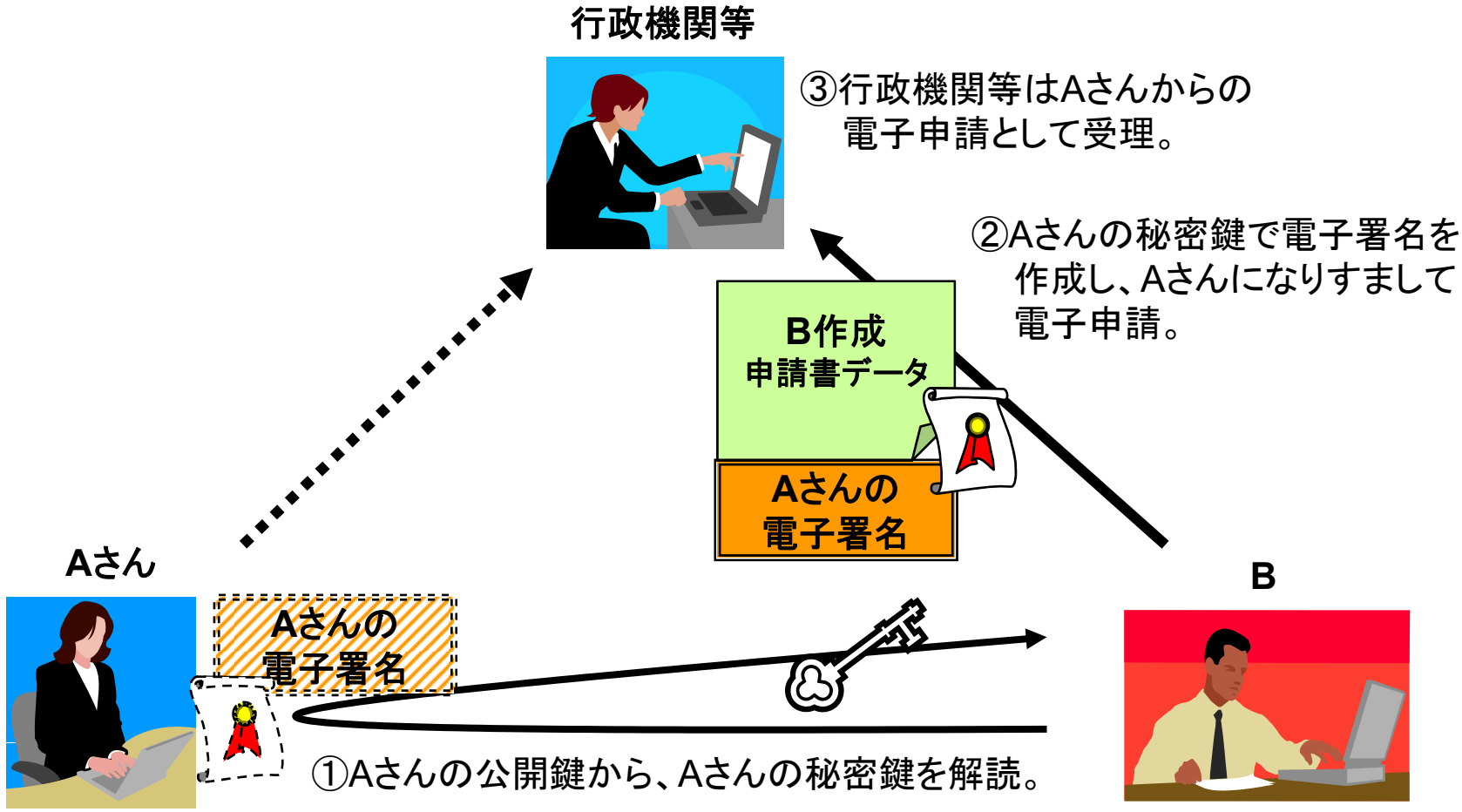
SHA-1の安全性低下により、将来異なる電子文書から同一のメッセージダイジェストが生成され、オンラインでの申請・届出等において申請書データの改ざんが行われる可能性がある。



参考資料

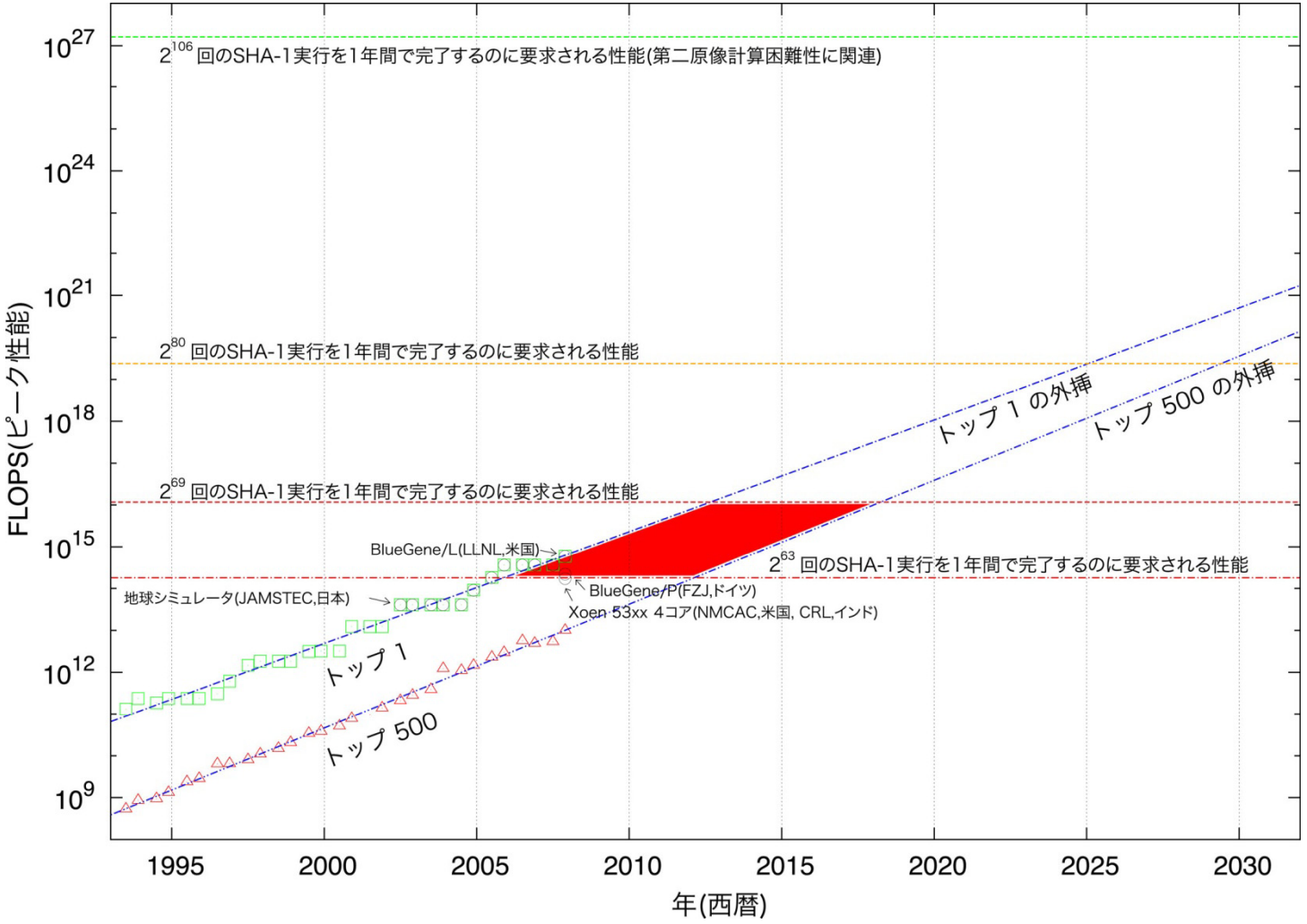
RSA1024の安全性低下について

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。



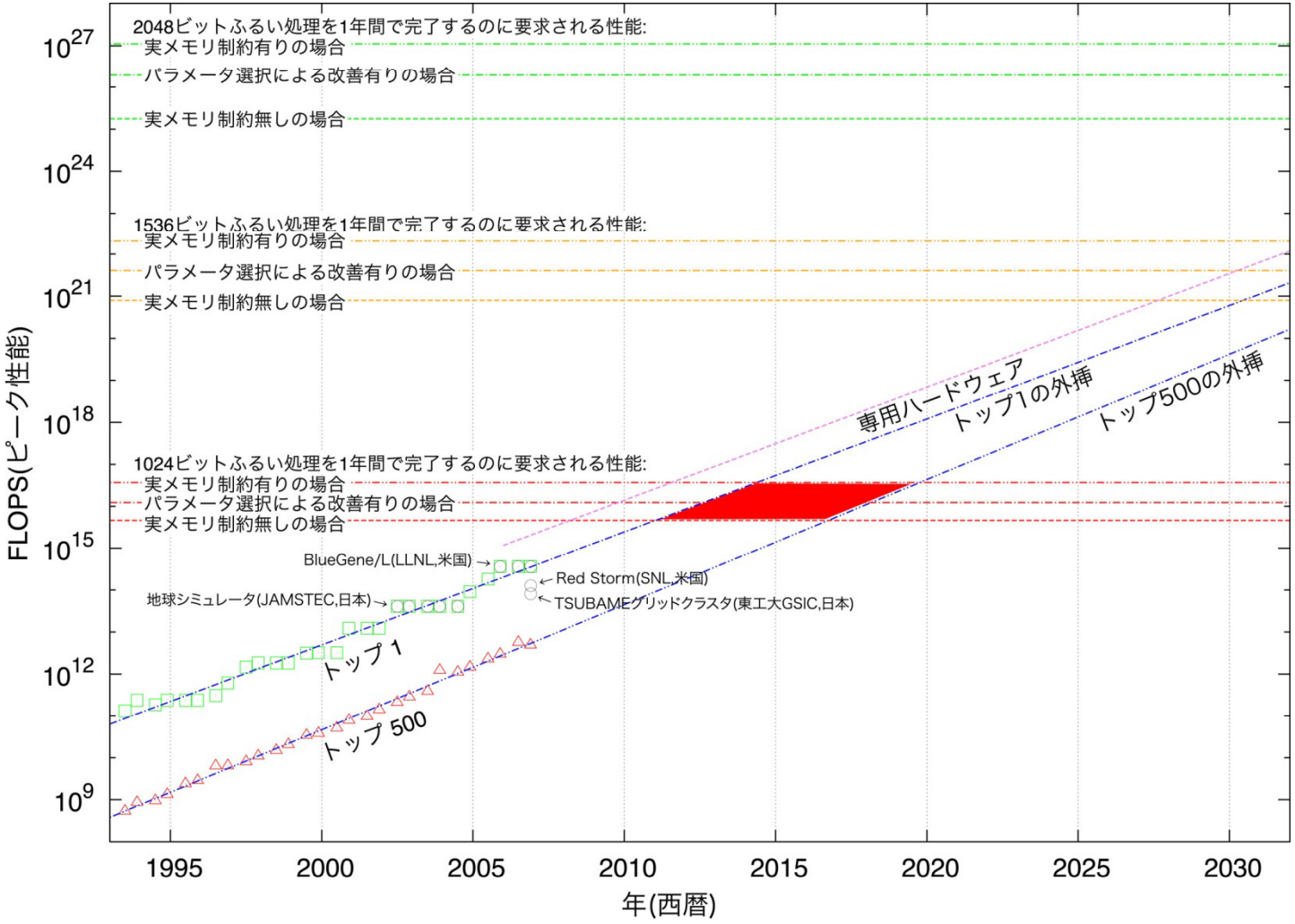
参考資料

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



参考資料

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



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（その２）

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）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。

- 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、SHA-1及びRSA1024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。
- 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。
- 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。
- 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。
- 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。

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（その３）

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）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。
- 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。
- 2014年度早期までに、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年度末前後を目途に、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。

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（その４）

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。

- 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を踏まえ、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は必要。

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（その１）

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。
- 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、」「暗号の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p.12を参照のこと。）。

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 1）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 1）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。