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

総務省 地域力創造グループ 地域情報政策室

検討会の開催背景

公的個人認証サービスにおいて利用し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、暗号技術検討会等はその安全性に懸念が生じる可能性を指摘している。

※ 暗号技術検討会は、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が開催。

当該指摘も踏まえ、情報セキュリティ政策会議、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等においては、新たな暗号方式等への移行について検討が行われている。

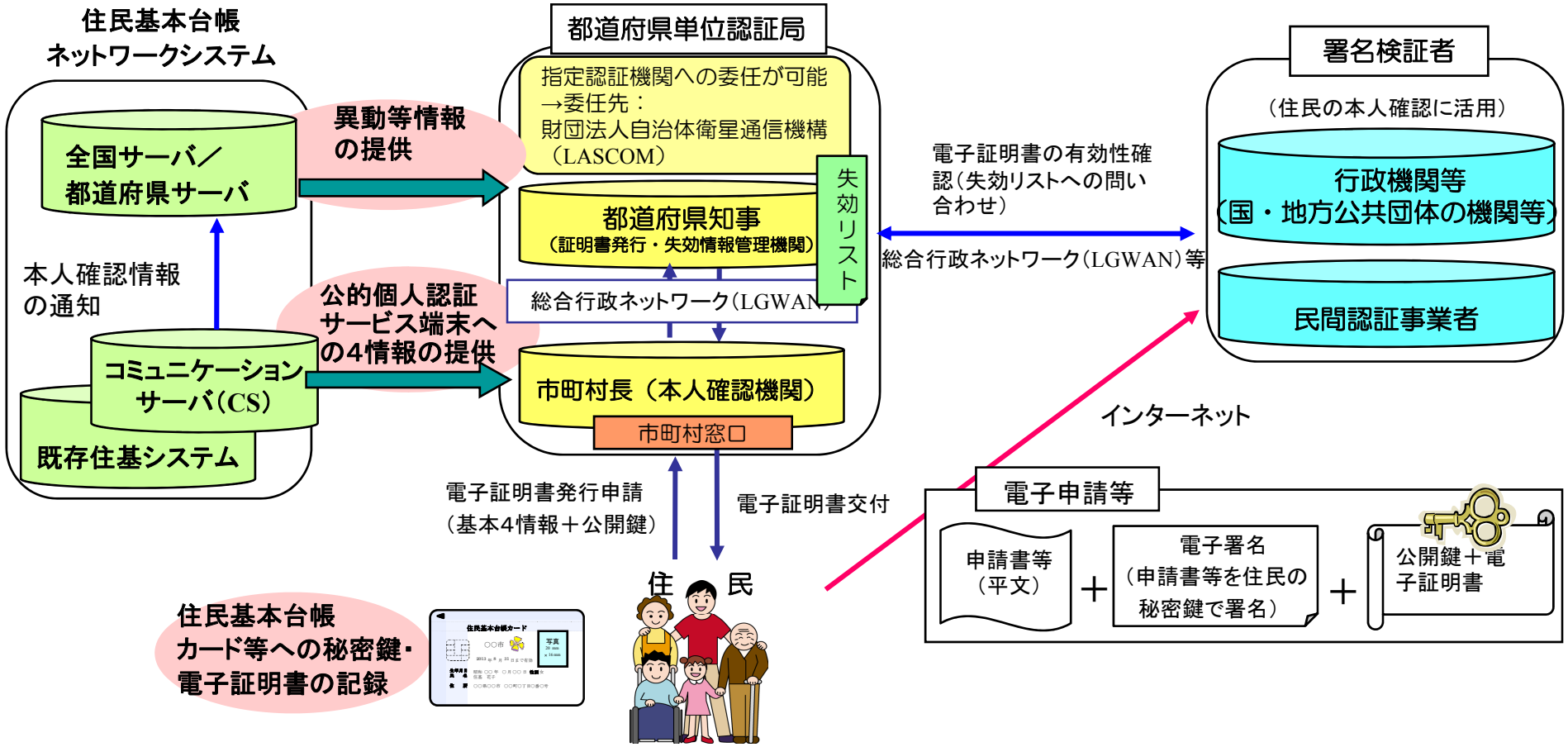
※ 政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針（平成20年4月22日情報セキュリティ政策会議決定）

※ 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）

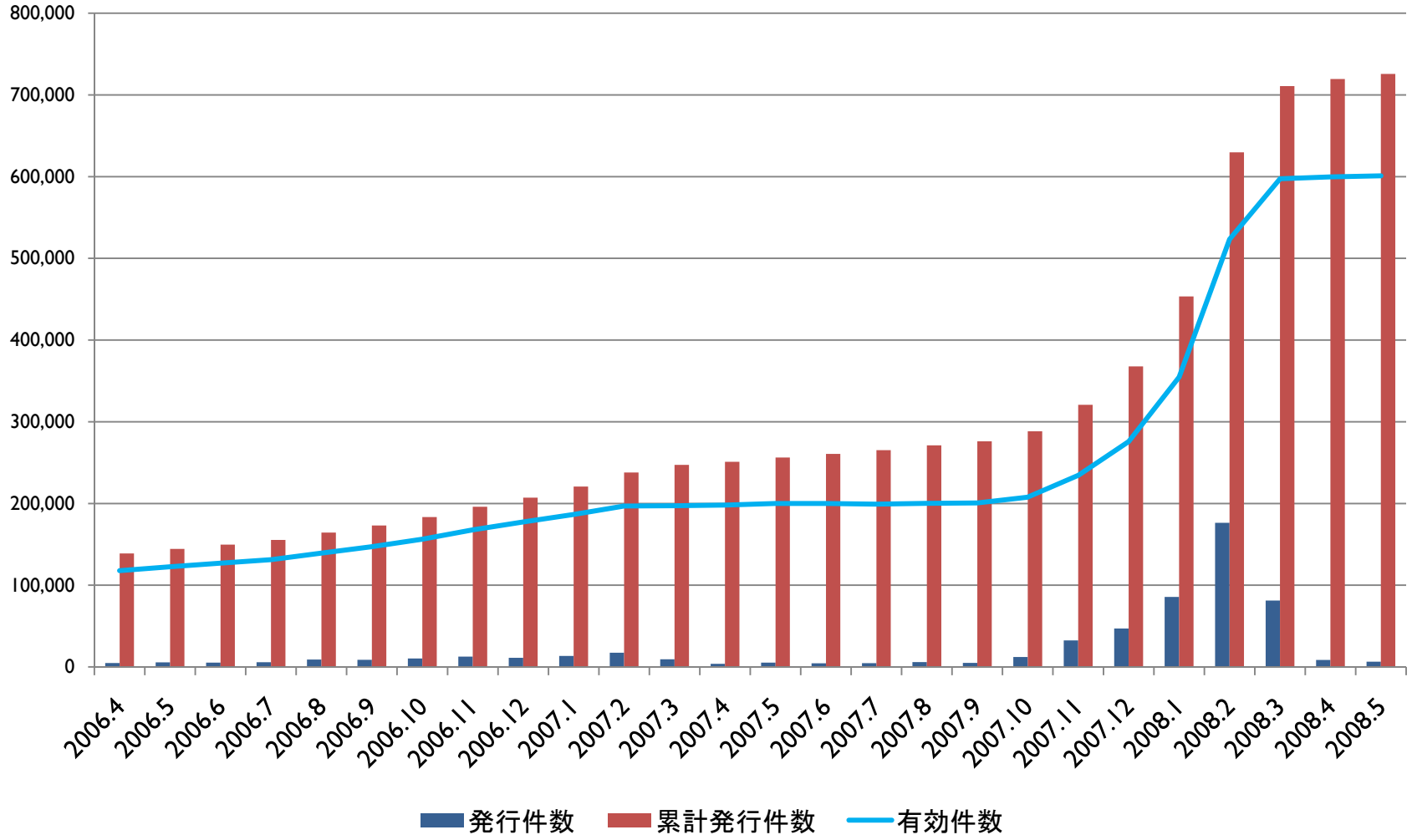
このため、公的個人認証サービスについても、その信頼性を引き続き確保するため、「公的個人認証サービスにおける暗号方式等の移行に関する検討会」を開催し、暗号方式等の移行について学識経験者・関係機関等による検討を行う。

公的個人認証サービス

○　オンラインでの行政手続等における本人確認のためのしくみ。
○　なりすまし、改ざん、送信否認などを防ぐため、高いセキュリティを確保。
○　電子証明書の発行件数：約71万件（2007年度末）



電子証明書の発行枚数


800,000
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
2006.4
2006.5
2006.6
2006.7
2006.8
2006.9
2006.10
2006.11
2006.12
2007.1
2007.2
2007.3
2007.4
2007.5
2007.6
2007.7
2007.8
2007.9
2007.10
2007.11
2007.12
2008.1
2008.2
2008.3
2008.4
2008.5
発行件数
累計発行件数
有効件数

法律、政令、省令及び告示（その１）

- 電子署名に係る地方公共団体の認証業務に関する法律（以下「法律」という。）

  第2条（定義）　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（平成十二年法律第百二号）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。

- 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（以下「省令」という。）

  第2条（電子署名の基準）

  法第二条第一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。

- 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（総務省告示）（以下「告示」という。）

  第2条（電子署名に係る基準）

  規則第二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。

法律、政令、省令及び告示（その２）

- 法律第3条（電子証明書の発行） 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（電子証明書の発行の方法等） 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。

- 告示第8条（発行者署名符号を作成する電子計算機等の基準） 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。

法律、政令、省令及び告示（その３）

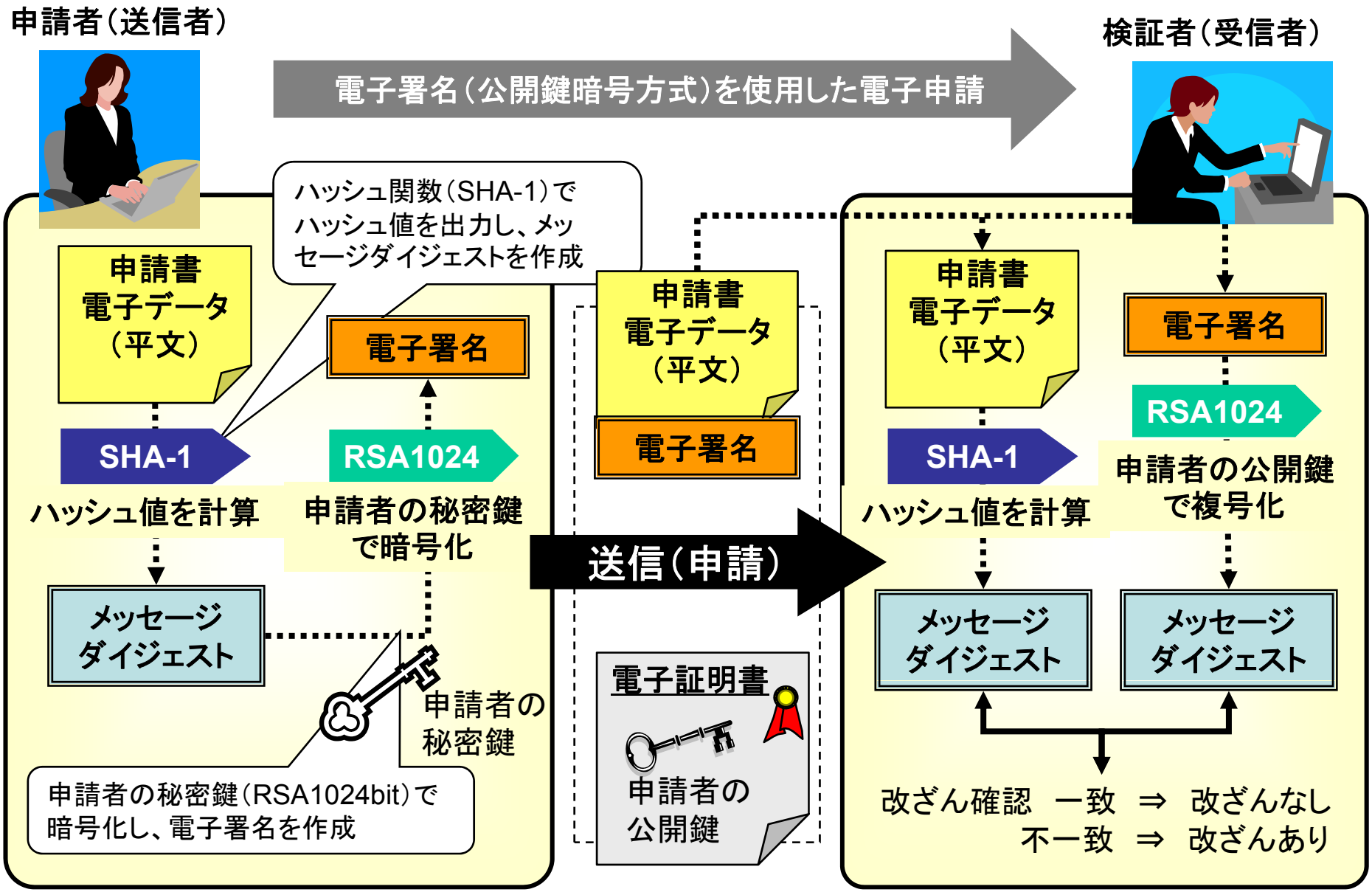
- 法律第17条（都道府県知事への届出等） 第1項　第5号
  電子署名及び認証業務に関する法律第2条第3項に規定する特定認証業務を行う者であって政令で定める基準に適合するものとして総務大臣が認定する者

- 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
  第8条（特定認証業務を行う者に係る認定の基準） 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（特定認証業務におけるその他の業務の方法） 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。

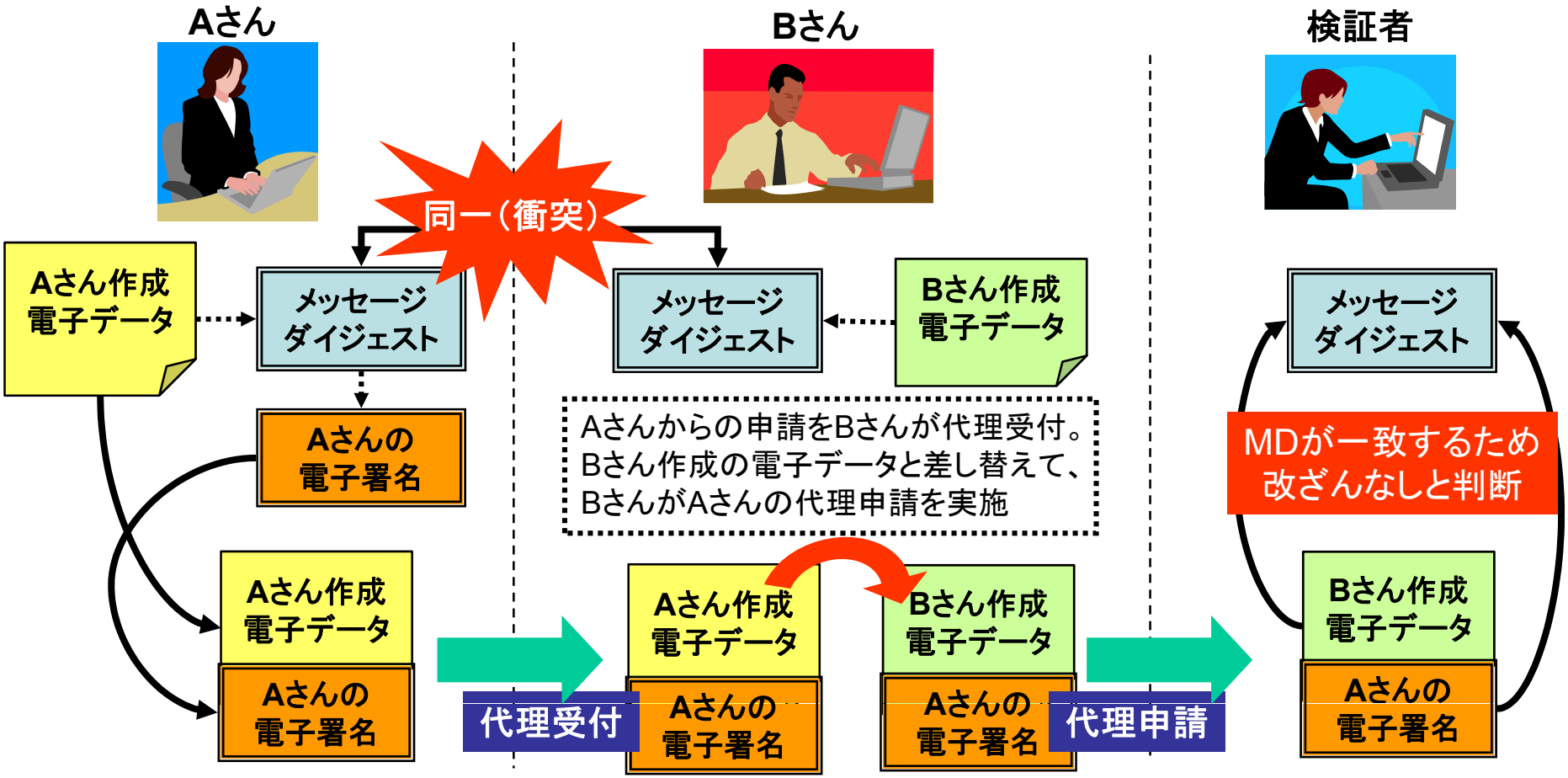
- 告示第31条（特定認証業務と他の業務との誤認を防止するための措置） 第2号
  発行者署名検証符号（電子署名及び認証業務に関する法律施行規則第六条第九号に規定する発行者署名検証符号をいう。次条において同じ。）に係る電子証明書の値をSHA―1で変換した値によって当該特定認証業務を特定すること。

ハッシュ関数及び公開鍵暗号方式を利用した電子署名の仕組み



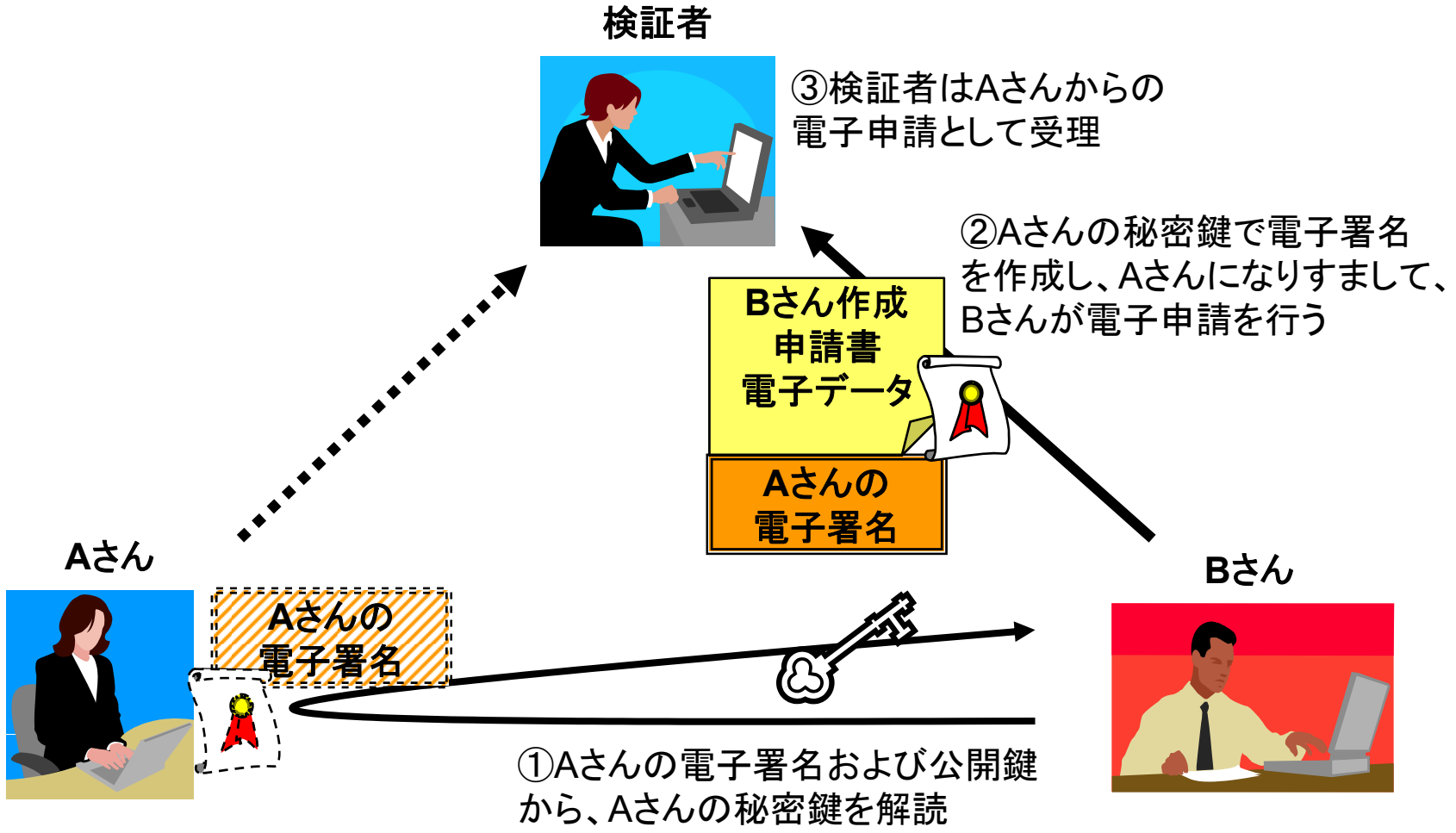
ハッシュ関数SHA-1の安全性低下について

ハッシュ関数の安全性が低下した場合、異なる電子データから同一のメッセージダイジェスト（MD）が生成される可能性がある。ただし、現時点では意図的な文書を同一のMDに変換することは困難。

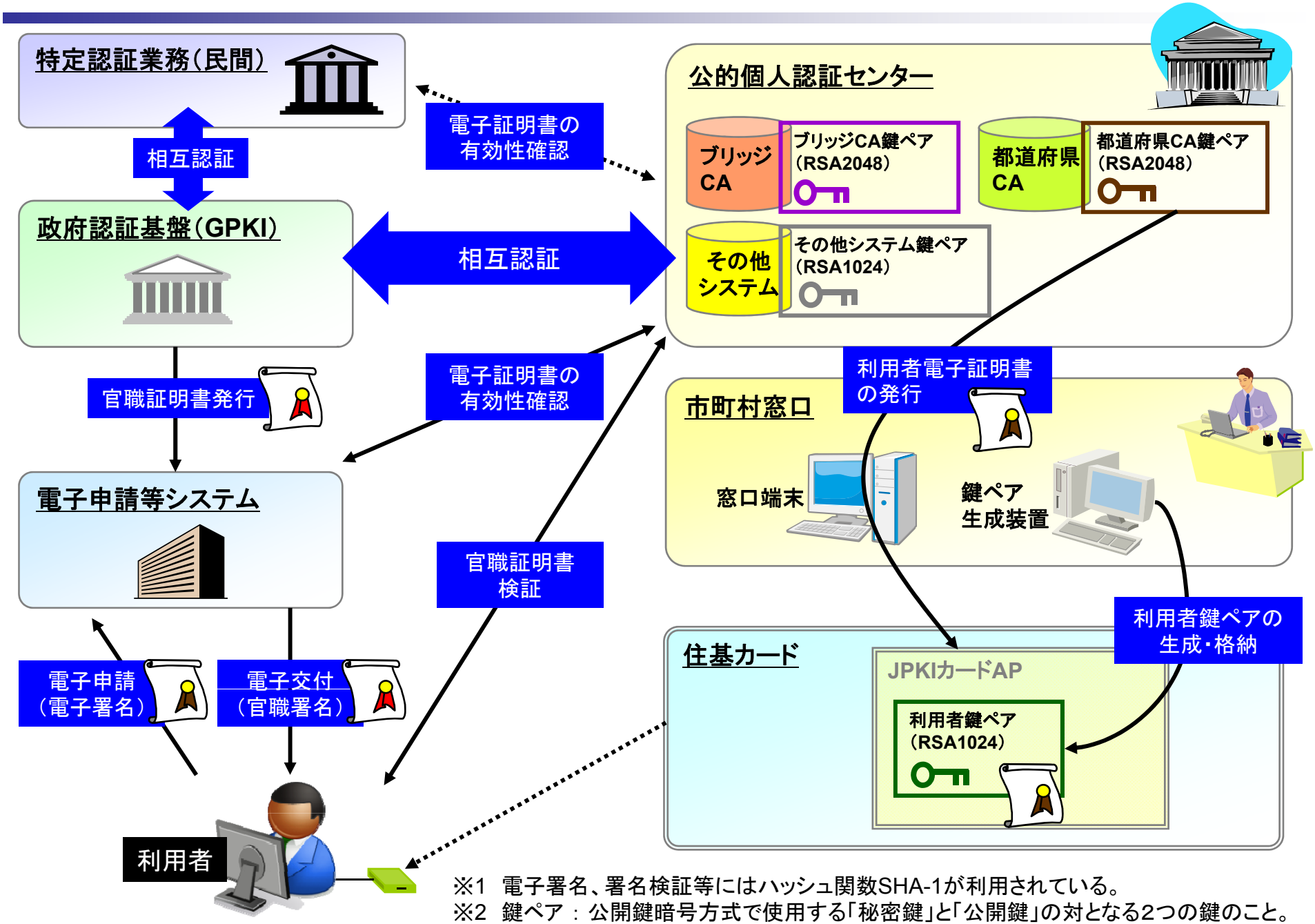


公開鍵暗号方式RSA1024の安全性低下について

公開鍵暗号方式の安全性が低下した場合、電子署名及び公開鍵から秘密鍵が解読されるリスクが発生し、電子申請において改ざんやなりすましが行われる可能性がある。



公的個人認証サービスにおける暗号方式等の利用について



※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。

検討会の進め方

検討事項	第1回 （9月16日）	第2回 （10月中下旬を予定。）	第3回 （12月中旬を予定。）
関係機関ヒアリング	●	●	
暗号方式等の移行の必要性について		●	
ハッシュ関数SHA-1及び公開鍵暗号方式RSA1024に代わる暗号方式等について		●	
暗号方式等の移行プランについて		●	●
移行に当たっての留意事項			●