資料１－６

電子署名及び認証業務に関する法律に係る課題について

平成１９年１２月１８日
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
経済産業省商務情報政策局情報セキュリティ政策室

電子署名法に係る課題

主務省が、有識者、認証事業者等の意見を聴取した際に提案された課題

Ⅰ．今回の検討会で検討事項とする課題：

1．技術的論点
　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．制度的論点
　認定認証業務における利用者の真偽の確認について
3．ビジネス的論点
　特定認証業務の認定制度の運用について

→ 何らかの具体的措置を速やかに検討すべきもの

Ⅱ．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について
2．認定制度の複数レベル化について
3．電子署名の長期検証性の確保について
4．認定認証業務の電子証明書に記載する属性情報について
5．利用者及び署名検証者による適切な電子署名の利用について
6．認定認証業務間でのブリッジ認証局の構築について

1．技術的論点

○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

○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RSA(1024bit)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。

※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

○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、特定認証業務の技術基準に、**どのような新暗号技術を追加すべきか**。

→SHA-1に代わる暗号として、SHA-2（SHA-256、SHA-384、SHA-512）？

→RSA1024bitに代わる暗号として、RSA1156bit,1408bit,1984bit,2048bit,ECDSA？

●**SHA－１**withRSA1024bit**による新規の電子署名が無効となる旨、どのように規定すべきか。**

→暗号技術検討会等と連携しながら検討

（参考）

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）（抄）

（特定認証業務に係る電子署名の基準）

第3条　規則第二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。

一　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

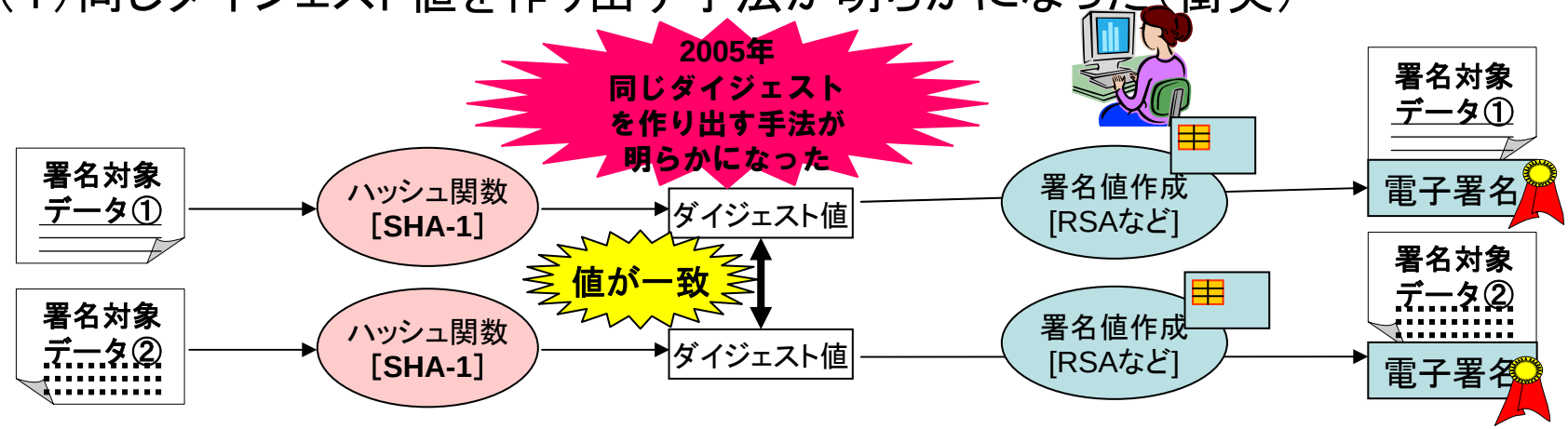
二　ECDSA方式（オブジェクト識別子　1　2　840　10045　4　1）であって、楕円曲線の定義体及び位数が160ビット以上のもの

三　DSA方式（オブジェクト識別子　1　2　840　10040　4　3）であって、モジュラスとなる素数が1024ビットのもの

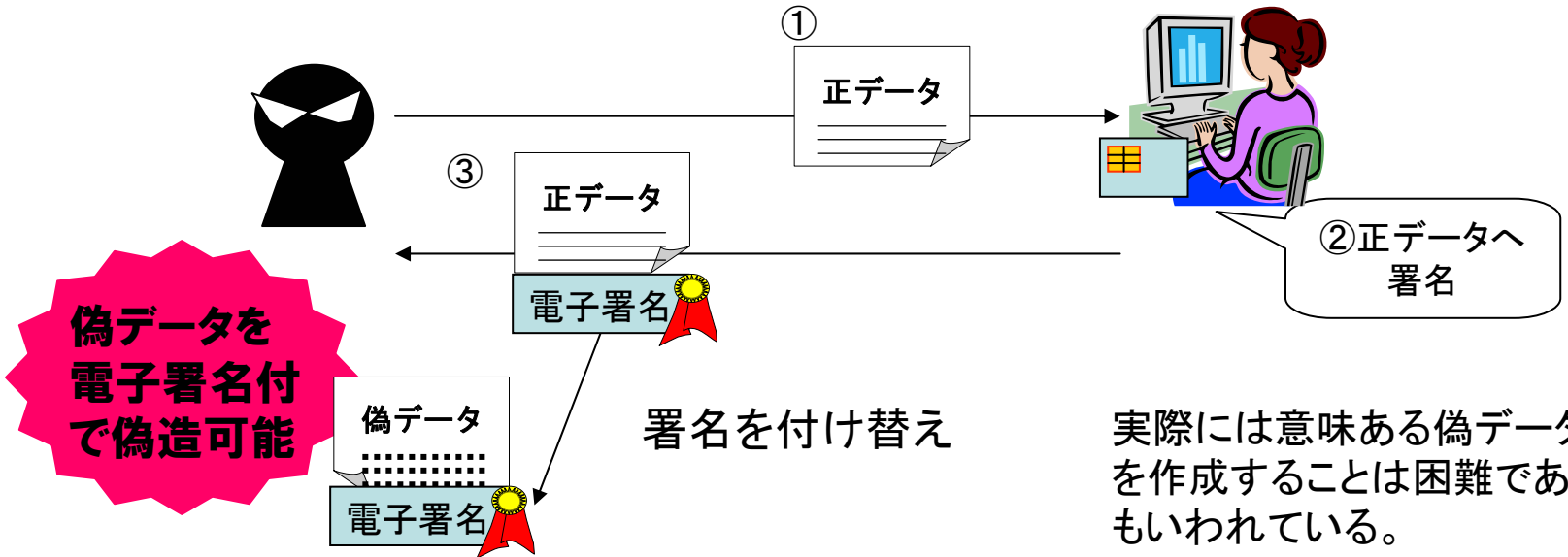
ハッシュアルゴリズムの安全性に係る状況（SHA-1）

非可逆（一方向）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）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



ハッシュアルゴリズム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）

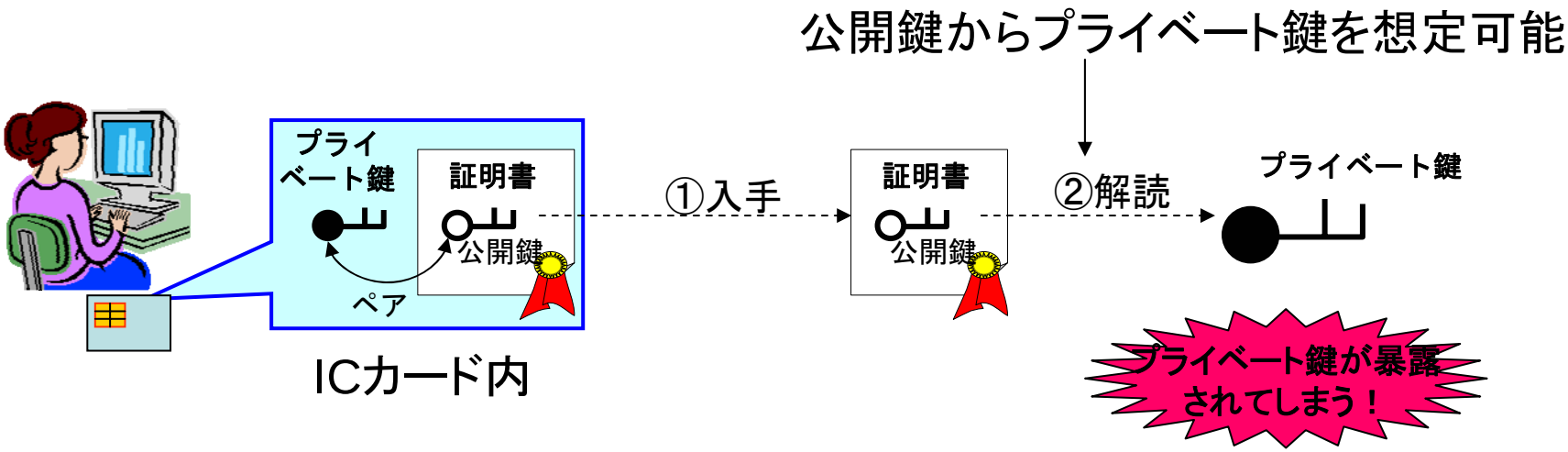
SHA-1の実行回数	2006年4月現在
2^{80}回(総当たり)	・国内最高速のスパコンで約100万年
新たな計算 ↓ 方法の発表	↓
2^{69}回	・国内最高速のスパコンで約462年以下

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

RSAアルゴリズム危殆化の影響

- RSAアルゴリズムにおいては、素因数分解によって「秘密鍵」が暴露されることで危殆化。
- 秘密鍵が暴露される→秘密鍵が偽造できる
- 公開鍵暗号方式で秘密鍵の偽造は致命的
  - 利用者の署名を偽造できる（利用者のプライベート鍵が漏えい）
  - 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



2. 制度的論点

○認定認証業務における利用者の真偽の確認について

○論点：

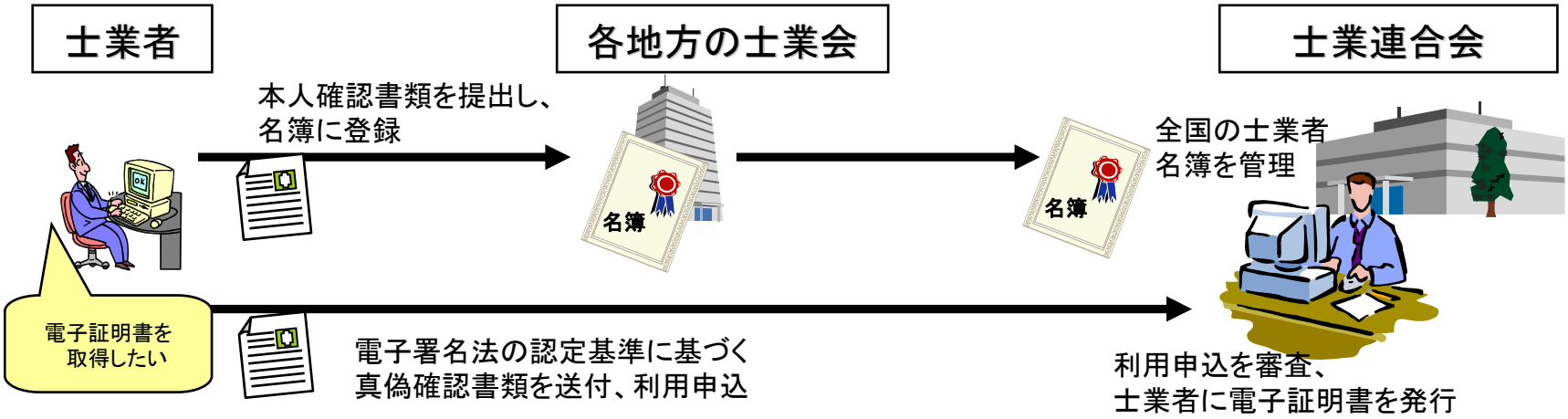
認定認証業務においては、電子証明書の発行に際して、次ページのような利用申込者の真偽確認を行うことが定められている。認定認証事業者でもある**全国社会保険労務士会連合会、日本税理士会連合会、日本司法書士会連合会、日本土地家屋調査士会連合会は、各士業関係法に基づき整備された名簿を管理**しており、**この名簿を利用して認定認証業務の真偽確認を簡略化できないか**という提案を行っている。電子政府評価委員会においても、同様の指摘がなされている。

○検討すべき事項：

●法令等に基づき整備された名簿等が認定認証業務における利用者の真偽確認の手段として利用可能か否か。

●課題を整理した上で、必要に応じて施行規則改正の必要性等今後の対応の方向性等を検討。

現在の士業連合会における認定認証業務イメージ



（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

＋

※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1－A

・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
のうちいずれか1以上の提示

※例： 運転免許証、船員手帳、海抜免状、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

タイプ1－B

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

※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

タイプ1－C

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
(1) タイプ1－Aに掲げる書類のうち1以上
(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
(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）で写真付きのもののうち1以上

●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

3. ビジネス的論点

○特定認証業務の認定制度の運用について

○論点：

指定調査機関は現在、
・財団法人日本品質保証機構（略称：JQA）
・財団法人日本情報処理開発協会（略称：JIPDEC）
の2機関であるが、今後業務を継続していくためには調査業務の更なる効率化や調査手数料の見直し等が必要となる。

認定認証事業者の負担増は避けられないが、その一方で、電子署名を一般化させる工夫が必要ではないか。

○検討すべき事項：

●電子署名の利用促進策について

電子署名を身近なものとするため、ニーズを把握しつつ、一層の普及促進策を実施すべきではないか。