資料6

「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

～電子署名法検討会　報告書概要～

平成20年9月

電子署名法主務三省
（総務省、法務省、経済産業省）

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　概要

開催目的

「電子署名及び認証業務に関する法律」（電子署名法）は、平成１２年第１４７回国会の審議を経て、同年５月に公布、平成１３年４月１日に施行された。

電子署名法附則第3条においては、施行後5年を経過した場合に、同法の施行の状況について検討を行うものとされており、総務省、法務省及び経済産業省は、平成18年度以降、外部有識者のヒアリングを行うなどして同法施行上の課題の抽出等を実施してきた。

この検討会は、当該抽出した課題について議論を行い、今後の電子署名法の運用に反映していくため、開催したものである。

開催時期

第１回　平成１９年１２月１８日
第２回　平成２０年２月１９日
第３回　平成２０年３月３１日

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　構成員・オブザーバ名簿

（構成員）

石黒　義昭　　株式会社コンストラクション・イーシー・ドットコム　代表取締役常務

澁谷　裕以　　社団法人日本経済団体連合会情報通信委員会情報化部会ITガバナンスWG　委員

高橋　伸和　　日本ベリサイン株式会社　顧問

辻井　重男　　情報セキュリティ大学院大学　学長

手塚　悟　　株式会社日立製作所システム開発研究所情報サービス研究センタ シニアマネージャ

西村　達之　　セコムトラストシステムズ株式会社　代表取締役副社長

早貸　淳子　　情報セキュリティ大学院大学セキュアシステム研究所　客員研究員

藤原　宏高　　日本弁護士連合会コンピュータ委員会　委員

松本　恒雄　　一橋大学大学院法学研究科　教授

満塩　尚史　　ディーディーエヌコンサルティング株式会社　ディレクター

（オブザーバ）

伊藤　毅志　　内閣官房情報セキュリティセンター　参事官

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　センター長

塚田　桂祐　　総務省大臣官房　参事官

中井川　禎彦　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　管理官

山内　徹　　内閣官房IT担当室　内閣参事官

（敬称略・五十音順）

電子署名及び認証業務に関する法律（電子署名法）の枠組み

（平成12年5月31日法律第102号、一部の規定を除いて平成13年4月1日から施行）

電磁的記録の真正な成立の推定

電子署名の法律上の取扱いを明確化する

本人による一定の条件を満たす電子署名が付されている電子文書等の真正な成立の推定（第3条）

特定認証業務に関する認定の制度等

信頼できる認証業務に対する認定制度を導入する

① 認証業務の認定（第4条～16条）
② 指定調査機関等（第17条～32条）
③ 雑則（第33条～40条）
④ 罰則（第41条～47条）

↓

電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進

↓ 電子商取引等のネットワークを通じた社会経済活動の更なる発展

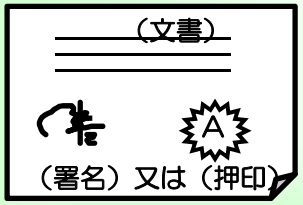
国民生活の向上及び国民経済の健全な発展

電磁的記録の真正な成立の推定

［手書き署名・押印］

○　民事訴訟法第228条第4項

「私文書は、本人又はその代理人の**署名又は押印**があるときは、**真正に成立したものと推定**する。」



「本人の署名又は押印」　があるときは、

文書の真正な成立（本人の意思に基づき作成されたこと）の推定

類似の仕組みを導入

［電子署名］

○　電子署名及び認証業務に関する法律第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。」

「本人による一定の条件を満たす電子署名」がされているときは、

電磁的記録の真正な成立の推定

特定認証業務に関する任意的認定制度

任意の認定制度の創設の趣旨

民間の認証業務の健全な発展のため、本人確認の方法等が信頼できるかどうかを国民が判断できる目安を示す制度を導入。

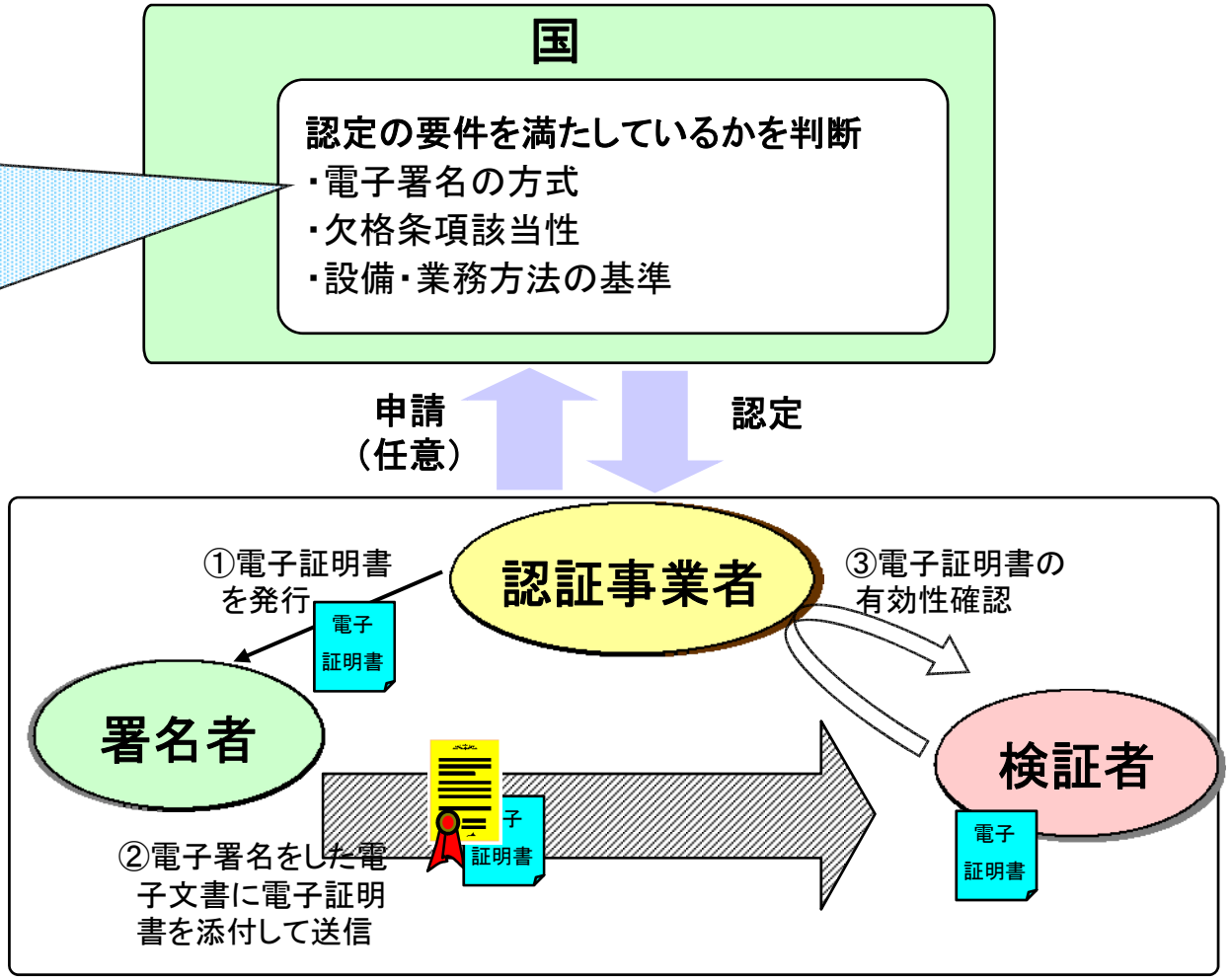
【電子署名の方式】

特定認証業務

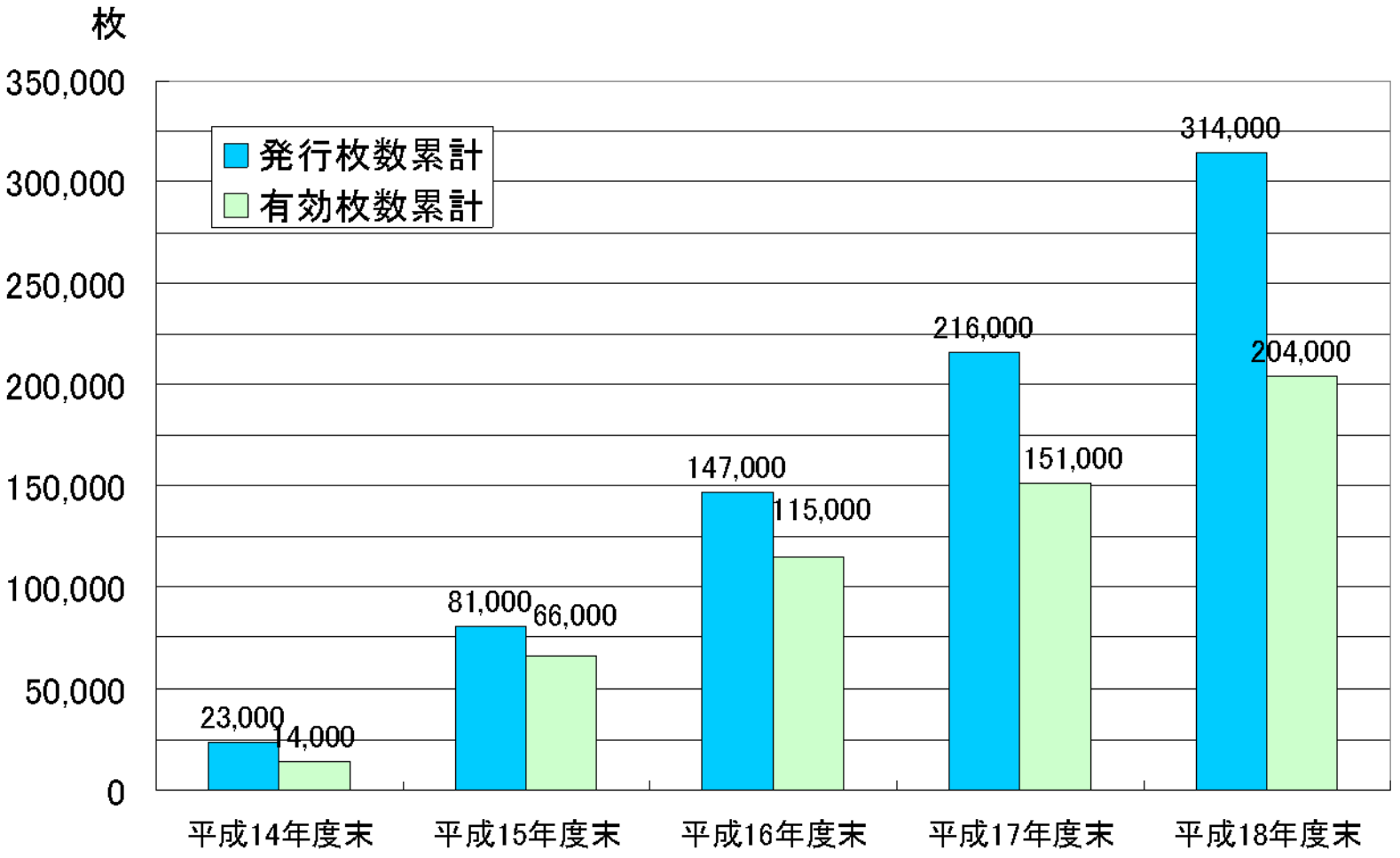
電子署名のうち、本人だけが行うことができるものとして、次の基準のいずれかに適合する電子署名について行われる認証業務

- RSA 又はRSA－PSS，1024bit以上
- ECDSA，160bit以上
- DSA，1024bit以上

※　認定の審査に当たって必要となる業務の実施体制の実地調査は、**指定調査機関**が行う。



認定認証事業者による電子証明書の発行状況



注1：廃止された認定認証業務に係る電子証明書の発行枚数を含む。
注2：数字は概数である。

【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のうち、ハッシュ関数SHA-1及び公開鍵暗号RSA1024bitについては安全性の低下が指摘されているが、どのような対応を採るべきか。

・検討事項

SHA-1、RSA1024bitを用いた新規電子署名の中止を見据え、指針第3条で規定する特定認証業務に係る電子署名の基準に、どのような電子署名の方式を追加すべきか。

・検討結果

告示第3条（特定認証業務に係る電子署名の基準）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を追加し、SHA-2及びRSA2048bit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。（今後、告示の改正を予定。）

本検討会の検討結果（暗号アルゴリズムの移行部分抜粋）
電子署名に用いる暗号技術の安全性向上に係る方策（技術的論点）

・検討事項

SHA-1、RSA1024bitを用いた新規電子署名の中止を見据え、指針第3条で規定する特定認証業務に係る**電子署名の基準からSHA-1、RSA1024bitを用いた電子署名の方式を削除することを含め、どのような措置をどのようなスケジュールで行うべきか。**

・検討結果

主務省においては、**以下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**。また、今後主務省は、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**。

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） *政府機関システム移行指針（案）による
（2013年度）	（政府機関システム新旧暗号アルゴリズム（SHA-1及びSHA-2、RSA1024bit及び2048bit）対応環境構築が完了） *政府機関システム移行指針（案）による
2013年度末まで	認定認証事業者に対して、暗号移行に係る変更認定のための調査が必要な場合は実施し、認定認証事業者は、RSA2048bitを用いた発行者鍵ペアを新たに生成する必要がある場合は、生成。
2014年度 早期まで	認定認証事業者は、RSA2048bitによる発行者鍵ペアを活性化させ**SHA-2及びRSA2048bit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、RSA1024bit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、RSA1024bitを削除。** （SHA-1、RSA1024bit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、RSA2048bit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。）