別紙

提出された意見とこれらに対する考え方

＜提出順＞

提出された意見	考え方
標記指針の一部改正案は、最新の暗号技術動向等を踏まえた検討の結果として改正されるものであり、その趣旨については、十分に理解できるものと考えます。 また、本改正案は、現在規定されている電子署名の方式において用いられている暗号技術に、新たに SHA-2 及び RSA2048 を追加するというものであり、現行の暗号技術である SHA-1 及び RSA1024・2048 が使用できなくなるものではないという点において、適切な取扱いであるものと考えます。 しかしながら、SHA-2 及び RSA2048 へ移行するためには、移行に要する費用、移行に関する検討及び移行の諸準備に要する時間が必要であり、移行に要する期間が十分でないと、円滑な切替が行えず、運用に支障を来たすことが予想されます。 したがいまして、現行の暗号技術である SHA-1 及び RSA1024 を、今後 20 年程度（2030 年頃）まで、SHA-2 及び RSA2048 と並行して用いることができるよう要望いたします。 （日本土地家屋調査士会連合会）	暗号アルゴリズムの移行については、「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）」を踏まえ、具体的な告示の改正については、過去の事例を参考にしつつ、進めていくことを考えております。 なお、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の移行については、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 日決定）が示され、検討が進められているところであり、政府機関と相互認証している認証局等においては、情報セキュリティ政策会議の動向や政府認証基盤（GPKI）での検討状況等を踏まえておく必要があるものと考えます。
既存のアルゴリズムの証明書から、新しいアルゴリズムの証明書への移行方法について明確にする必要がある。 ＜理由＞ 利用者証明書や認証局証明書の移行について、利用者である国民の手間や認定認証事業者の作業が最小限となるよう、アルゴリズム移行の方法を検討し明確に情報発信する必要があると考えます。 利用者証明書と認証局証明書では、アルゴリズム脆弱性による影響が異なるため、移行対応の方法についても分けて考える必要があります。 また、認証局証明書の移行は、認証局の鍵更新を伴い実施することが考えられますが、現在の認証局の鍵更新については、新認証局と旧認証局の双方ともに共存しなければ鍵更新が行なえない状況であり、2 つの認証局の運用コストや、データの整合性をとるための作業実施や、新認証局の認定までの間のサービス提供停止等の影響が発生する	御意見については、今後の暗号アルゴリズムの移行の際に、参考とさせていただきます。なお、暗号アルゴリズムの円滑な移行に向け、必要な検討を進めていくとともに、情報提供に努めてまいります。

ため、効率的な認証局の移行についての検討が必要と考えます。 （セコムトラストシステムズ株式会社）	
政府認証基盤等を含め政府として統一的なアルゴリズム移行対応のスケジュール（新アルゴリズムの証明書発行開始と旧アルゴリズムの証明書の終了時期）を明確にする必要がある。 ＜理由＞ 新しいアルゴリズムの証明書を利用者に提供するには、主な利用先である政府アプリケーションが新アルゴリズムへの対応を完了している必要があります。新たなアルゴリズムの証明書の提供開始から、旧アルゴリズムの証明書が存在してもよい新旧アルゴリズムが共存する移行期間が明確でないため、現在の旧アルゴリズムの有効期間 5 年の証明書を何時まで発行してよいのか判らない。認定認証事業者のサービス提供に影響を及ぼすため、政府内で統一したスケジュールを早急に提示する必要があると考えます。 （セコムトラストシステムズ株式会社）	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の移行については、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 日決定）が示されており、当該移行スケジュールの検討状況については、内閣官房情報セキュリティセンター（NISC）から、第２０回情報セキュリティ政策会議に「『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』に基づく検討状況について」の中で報告されております。
アルゴリズムの移行に関してコストが最小限となるよう考慮が必要である。 ＜理由＞ 既存の認証業務と新しいアルゴリズムの認証業務がそれぞれ異なる特定認証業務として扱われた場合、認証事業者は 2 重の運用コストが発生し事業運営への影響やサービス提供料金への影響が考えられます。 また、利用者が保有する証明書を新アルゴリズムへ切り替えを希望する場合、審査書類の準備の手間や再取得のための証明書費用の発生が考えられます。 コストが最小限ですむよう、効率的なアルゴリズム移行の方法や、利用者への費用補助等、利用促進の足枷とならないよう費用面での配慮を行うことが重要であると考えます。 （セコムトラストシステムズ株式会社）	御意見については、今後の暗号アルゴリズムの移行の際に、参考とさせていただきます。 なお、前述の通り、暗号アルゴリズムの円滑な移行に向け、必要な検討を進めていく予定でありますが、その際には暗号移行作業の効率性にも留意しつつ進めていく予定です。