

「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」の一部を改正する告示案に対する意見募集結果

意見(全文)	考え方
<p>日本土地家屋調査士会連合会(以下、「日調連」という。)は、現行の電子署名及び認証業務に関する法律(以下、電子署名法という。)に基づき、認証業務及びこれに附帯する業務に関する技術基準(平成15年総務省告示第706号)を踏まえて、平成17年12月9日付で、総務省・法務省・経済産業省の認定を受けて、日本土地家屋調査士会連合会認証サービス(以下、「日調連認証局」という。)を開設・運営するものである。</p> <p>日調連認証局にあつては、日調連が定める特定認証局運用規程(「CPS」と称する。)の「証明書の鍵更新」においては、CA秘密鍵(「認証局秘密鍵」という)の更新を5年ごとに行うと定めており、平成22年秋にこの更新時期を迎える事情にある。</p> <p>今般、委託業者に、この更新に係る費用を見積もらせたと、開設時の認証局システム構築費を上回る改修費用額を提示され、戸惑いを覚えたところである。</p> <p>委託業者から、仔細に説明を求めたところ、この改修費用には、現在の秘密鍵の暗号アルゴリズム(SHA-1及びRSA 1024)は、危殆化が急速に進んでいることから、新暗号アルゴリズムへの移行に備える経費を含めているとのことであった。</p> <p>新暗号アルゴリズムへの移行が必要となることは一応、理解できるものの、危険性が増すごとに、毎回、開設時の認証局システム構築費相当の予算を計上し続けなければならないことは、会費で予算が賅われている日調連のような組織にとっては、会員の理解が得られない事態が起きると危惧するところである。</p> <p>現在、新暗号アルゴリズムへの移行について、「電子署名法における暗号アルゴリズム移行研究会」で精力的に検討されていることは、承知しているが、移行に関する費用負担の当否について、十分な議論が尽くされているとは思えないとの認識を持っている。</p> <p>特に、国家戦略として情報化社会を実現する端緒として、行政手続の面から、多くの資格者団体の一員として、日本土地家屋調査士会連合会は、資格者を証明する必要性から、所属会員の負担を前提として、日調連特定認証局を構築し、運営を開始し、行政手続の円滑化へ一定の貢献をはたしてきたと自負している。</p> <p>このような背景を持つ日調連特定認証局とすれば、新暗号アルゴリズムへの移行の議論の方向によっては、組織の存続にも影響を与えかねないものとの強い危惧を感じているものである。</p> <p>ついては、このような検討会への参加の機会を設けられるなど、民間で運営されている特定認証局の運営実態を踏まえ、移行に要する費用の負担が相当であるかなどの議論の場が適切に設けられるよう要望する。</p> <p>(日本家屋調査士会連合会)</p>	<p>電子署名及び認証業務に関する法律に規定する認定認証事業者が使用する暗号アルゴリズムの移行については、同法を所管する行政機関において判断されるべきものと考えます。</p>