デジタル署名を利用する TSA 及び TA 業務に対する暗号アルゴリズム移行への検討開始のお知らせ

平成 22 年 7 月 8 日
財団法人　日本データ通信協会
タイムビジネス認定センター

安全性の低下が指摘されている RSA1024bit や SHA-1 等の暗号アルゴリズムに対応するため、電子署名法で規定する電子署名においてより強度の強い暗号アルゴリズム(SHA-2 及び RSA2048bit)へ移行する際のスケジュールが、内閣官房情報セキュリティセンター、総務省、経産省等で検討されています。

タイムビジネス認定センターでは、これらの状況を踏まえ、デジタル署名を使用する TSA 及び TA 業務において利用する暗号アルゴリズムをより強度の強い暗号アルゴリズムへ移行させるため、該当する基準改訂等の検討作業に着手しましたので、お知らせいたします。
タイムスタンプの有効期間の長さからできるだけ早期の移行が望ましいこと、また、現在のタイムビジネス関係事業者の検討状況、移行には一定の準備期間の必要なことなどを踏まえ、改訂した基準適用の目標期日は、2012 年 4 月 1 日を予定しています。

(参考)
TBF(タイムビジネス協議会)の「タイムビジネス暗号移行タスクフォース」では、デジタル署名を使用する方式に付き、TSA 及び TA 業務で利用する暗号アルゴリズムをより強度の強い暗号アルゴリズムへ 2012 年 3 月 31 日までに移行する方針で各種作業スケジュールの検討を進めています(詳細についてはこちらを参照)。