2011.02.10

タイムビジネス信頼・安心認定制度認定基準一部改定の概要

タイムビジネス認定センターでは、タイムビジネス信頼・安心認定制度認定基準の一部改定を予定しています。

これは、タイムビジネスに使用している暗号の脆弱化に対応するための暗号アルゴリズム移行と認定基準の明確化・現行化等ための見直しを目的としています。

今般、改定案が策定されましたので、広くパブリックコメントを募集します。

1. 暗号の脆弱化に対応するための暗号アルゴリズム移行に伴う改定

2010 年 7 月 8 日付の「お知らせ」で周知しました暗号アルゴリズム移行に対応するためのデジタル署名を使用する時刻認証業務の認定基準の改定箇所は、下表の通りです。

なお、「お知らせ」にもありますように本改定認定基準の適用日は、2012 年 4 月 1 日からを予定しています。

時刻認証業務(デジタル署名を使用する方式)認定基準改定案

グレー網掛け部:改定項目、下線部:追記箇所、取消線:削除

（1） 技術基準

項目	基準（遵守事項）
11 タイムスタンプの生成に関わる暗号技術	タイムスタンプの付与対象となる電子文書のハッシュ値を得るためのハッシュ関数、タイムスタンプのデジタル署名に用いる公開鍵暗号技術は以下の条件を満たすものを使用すること
2 タイムスタンプのデジタル署名に用いる公開鍵暗号技術	タイムスタンプの生成に関わる公開鍵暗号技術は、電子政府推奨暗号リスト（暗号技術検討会2002年度報告書を踏まえ、平成15年2月20日に総務省、経済産業省が公表したもの）に記載された公開鍵暗号技術~~で確認される安全性以上のものとすること~~を用いること ただし、上記電子政府推奨暗号リストの署名アルゴリズムのうち、SHA系列についてはSHA-256ビット以上のビット長、RSAについては2048ビット以上のビット長のものを使用すること、また同署名アルゴリズムのうちRSAとは別のアルゴリズムを使用する場合は、SHA256 with RSA 2048ビットと同等以上の安全性を持つこと
13 タイムスタンプ生成に用いる秘密鍵に対する公開鍵証明書（TSA公開鍵証明書）	TSA公開鍵証明書は、以下の要件を満たすものであること
1 署名アルゴリズム	TSA公開鍵証明書及びそのルートCA証明書並びに中間CA証明書(使用している場合)の署名アルゴリズムとして、電子政府推奨暗号リスト（暗号技術検討会2002年度報告書を踏まえ、平成15年2月20日に総務省、経済産業省が発表したもの）に掲載された公開鍵暗号技術~~で確認される安全性以上のものをサポートすること~~を用いること ただし、上記電子政府推奨暗号リストの署名アルゴリズムのうち、SHA系列についてはSHA-256ビット以上のビット長、RSAについては2048ビット以上のビット長のものを使用すること、また同署名アルゴリズムのうちRSAとは別のアルゴリズムを使用する場合は、SHA256 with RSA 2048ビットと同等以上の安全性を持つこと

2. 基準の明確化・現行化等の見直しのための改定

基準の明確化・現行化等の見直しのための認定基準の改定箇所は、下記認定基準改定案の内、1. に挙げた 2 項目以外の箇所になります。

なお、本改定認定基準の適用日は、改定後適切な周知期間をおいたあととなります。

認定基準改定案

・時刻配信業務

・時刻認証業務（デジタル署名を使用する方式）

・時刻認証業務（リンキング方式）

・時刻認証業務（アーカイビング方式）

注 1) グレー網掛け部:改定項目、下線部:追記箇所、取消線:削除　黄色網掛け部:追加項目

注 2) 本基準では、従来、時刻配信局を「TA(Time Authority)」と記載していたが、今年度発行された ITU-R の勧告で時刻配信局が「TAA(Time Assessment Authority)」と定義された。このことを受け、本基準においても「TA」と記載されていたものを「TAA」と修正した。

3. パブリックコメントの募集

本認定基準改定案へのパブリックコメントは、3 月 9 日（水）までに下記 URL の認定センター問合せフォームへご提出下さい。

http://www.dekyo.or.jp/tb/inquiry/index.html

以上