

## タイムビジネス信頼・安心認定制度認定基準一部改定のお知らせ

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行います。この改定は、以下の3点を目的としたものです。

- (1) 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
- (2) 時刻配信業務の技術基準が JIS X 5094「UTCトレーサビリティ保証のためのタイムアセスメント機関(TAA)の技術要件」として制定されたことに伴い、当該基準のJISへの準拠
- (3) 認定基準の明確化・現行化等

### 1. 認定改定基準適用日

本改定による改定認定基準の適用日は、2012年10月1日とします。

なお、2010年7月8日「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」及び2011年2月10日「タイムビジネス信頼・安心認定制度認定基準の一部改定に関するパブリックコメントの募集」において、下記に記載の2.改定内容(a)及び(c)については、2012年4月1日を適用日とする予定としておりましたが、変更になりましたのでご承知おき下さい。

### 2. 改定内容

#### (a) 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

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「ただし書き」のとおりです。

#### 時刻認証業務(デジタル署名を使用する方式)認定基準改定箇所

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)	エビデンス例
	T1 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を使用すること  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	TSAポリシー、タイムスタンプトークン、安全性レベルの証明資料
	T3 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、経済産業省が公表したもの)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  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  注) なお、ルート証明書の署名アルゴリズムについては、当面の間、SHA-1の使用を認める。	TSA公開鍵証明書及び当該証明書に係るCP/CPS

(b) 時刻配信業務認定基準 JIS 準拠に伴う改定

JIS 準拠とするため、(1)技術基準は以下のとおり改定します。

(1) 技術基準

項目	基準（遵守事項）	エビデンス例
1 技術要件全般	JIS X 5094 7.2-7.5の要件を満たすこと ただし、7.2.2 c)、7.3.5及び7.4.5については、追記事項あり	
2 UTC (NICT)との時刻同期	JISX 5094 7.2.2 c)に記載の「ほかの時刻源」は、UTC (NICT)の異常検出が目的である	
3 TSA時計の時刻異常への対応	JISX 5094 7.3.5に基づくか、または配信先機器の稼働を停止する機能を用いること	システム機能説明資料
4 記録の保存	JIS X 5094 7.4.5に加えて下記の要件を満たすこと ①時刻差証明書及び時刻証明書の発行記録の保管期間が明確に定められていること ②時刻差証明書及び時刻証明書の発行記録の保存は適切な体制・方式で行い、改ざん防止機能あるいは改ざん検知可能な手段を用いること	TAAポリシー、時刻監査記録保管方法・体制の説明資料
5 時刻配信業務の通信に用いる暗号技術	時刻配信業務の通信路の安全性を公開鍵暗号技術または共通鍵暗号技術により実現する場合、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）に記載された暗号技術を用いること	TAAポリシー、安全性レベルの証明資料

参考：JIS X5094 (JISC HP 内 JIS 検索ページ) : <http://www.jisc.go.jp/app/JPS/JPS00020.html>

(c) 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、下記の認定基準改定箇所の内、上述の(a)、(b)に挙げた2項目以外の箇所になります。

認定基準改定箇所

- ・ 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（リンク方式）
- ・ 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) 時刻配信業務基準では、従来、時刻配信局を「TA(Time Authority)」と記載していましたが、ITU-R の勧告 (ITU-R TF. 1876 (03/2010)) で時刻配信局が「TAA(Time Assessment Authority)」と定義されました。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」と修正します。

なお、認定事業者の規程等において、従前の「TA」と記載されていたものは、「TAA」と読み替えます。

3. 改定認定基準

改定された認定基準は、以下のとおりです。

- ・ 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（リンク方式）
- ・ 時刻認証業務（アーカイビング方式）

以上