

お知らせ

ご利用者様各位

SII ●
セイコーインスツル株式会社
クロノトラスト部

〒261-8507千葉県千葉市美浜区中瀬1-8
TEL 043-211-7479
FAX 043-211-8019

件 名： 時刻監査証明書改修について

■概要

この度、弊社の時刻配信サービス（認定番号：TA0002）が発行する時刻監査証明書（TAC）の一部に、ASN.1符号化規則に合致しない箇所が判明しましたので、改修を実施いたしました。

弊社の時刻配信サービスを用いた時刻認証事業者のタイムスタンプサービスをご利用のお客さまにはご迷惑をお掛けいたしますが、現在ご使用のソフトウェアに影響が発生する場合には、弊社連絡先またはソフトウェア提供元までご連絡いただきますようお願い申し上げます。

■関連するタイムスタンプサービス

改修対象は、時刻配信サービス（認定番号：TA0002）で発行する時刻監査証明書ポリシー『0.2.440.200125.1.2.1』のTACです。次の時刻認証事業者が発行するタイムスタンプに含まれています。

- ・株式会社PFU 「PFUタイムスタンプサービス」（SD0002）
<http://www.pfu.fujitsu.com/tsa/>
- ・ドコモエンジニアリング北陸株式会社 「e-DCMタイムスタンプサービス」（SD0004）
<https://www.dcmtsa.net/index.html>

■発行済みタイムスタンプへの影響について

本件は、TACの符号化方法の誤りのみを是正するものです。TAC内に含まれる情報自体には欠落や改竄等の不備は無く、正しい値が格納されています。したがって、過去に発行されたタイムスタンプの信憑性を損なうことはございません。

■改修の詳細な説明

TAC内の属性情報（Attributes）のうち、6オクテットの固定長データとなっていた以下8箇所を3～6オクテットの可変長データに修正しました。

- | | |
|------------------------------|------------------------|
| ①offset major | : 上位時刻配信サーバとの時刻のずれの整数部 |
| ②offset fractionalSeconds | : 上位時刻配信サーバとの時刻のずれの小数部 |
| ③delay major | : 時刻監査時のネットワーク遅延の整数部 |
| ④delay fractionalSeconds | : 時刻監査時のネットワーク遅延の小数部 |
| ⑤maxOffset major | : 時刻監査規格(オフセット)の整数部 |
| ⑥maxOffset fractionalSeconds | : 時刻監査規格(オフセット)の小数部 |
| ⑦maxDelay major | : 時刻監査規格(ネットワーク遅延)の整数部 |
| ⑧maxDelay fractionalSeconds | : 時刻監査規格(ネットワーク遅延)の小数部 |

従来) 02 04 XX XX XX XX の6オクテット固定長データ

改修後) 02 0N XX XX XX XX の3～6オクテットの可変長データ

Nは1～4の値で後に続くデータの長さを示し、XXはデータの値により省略されます
例： [従来] 02 04 00 00 00 00 ⇒ [改修後] 02 01 00

■改修実施日

2008年5月26日（月）

■時刻監査証明書について

時刻監査証明書（TAC）とは、時刻配信事業者（TA）が、時刻認証事業者（TSA）でタイムスタンプに使用する時計の時刻を監査した結果を証明し、時刻のトレーサビリティを担保するX.509形式の属性証明書です。

■連絡先

セイコーインスツル株式会社 クロノトラスト部

TEL： 043-211-7479

（営業時間 9:00～18:00 当社休業日、土・日・祝祭日、年末年始を除く）

E-mail： chronotrust_help@sii.co.jp

ホームページ： <http://www.sii.co.jp/ni/tss/index.html>

以上