

日本のタイムスタンプの仕組みを世界に輸出

「電子文書の原本性保証に必要不可欠なタイムスタンプを、日本は世界に先駆けて制度化・実用化しました。この日本発の仕組みを世界中で活用できるよう標準化活動を行っています。」

岩間 司 (いわま つかさ)

電磁波計測研究所

時空標準研究室 研究マネージャー

本人かなりの引きこもり体質で、土日に家から一歩も外へ出ないことがままある。職場でも研究室と実験室にこもっているのを好むのだが、何の因果か毎年 ITU へ出席するためジュネーブへ飛ばされてしまう。しかしジュネーブでも会議以外では…。

● 電子文書に潜む脅威と今回の標準化のポイント

パソコンなどを使って作成するいわゆる電子文書は、何回複製（コピー）しても劣化の心配がなく、対応するソフトウェアさえあれば誰でも同じものを再現できることが大きな利点です。しかしながら、これは見方を変えると、元の文書を改ざんしたり、他人になりすまして文書を作成することも容易にできてしまうという欠点となります。これら電子文書の「改ざん」や「なりすまし」という行為はこれからのネットワークを中心とした情報流通社会においては大きな脅威となっています。

電子文書の改ざんやなりすましを防ぐために有効な手段として電子署名やタイムスタンプがあります。電子署名では「誰が」「何を」作成したかを証明することができ、タイムスタンプでは「い



つ」「何を」作成したかを証明できます。そして電子署名とタイムスタンプを併用することにより「いつ」「誰が」「何を」作成したか証明できることになります(図1)。

電子署名やタイムスタンプ付与の方法は、すでに標準化されており、特に電子署名については日本をはじめ各国で法制化されています。タイムスタンプについては、付与と並んで時刻の信頼性というもう1つの重要なファクタがあります。しかしながら、この信頼性については、協定世界

時(Coordinated Universal Time: UTC)にトレサブル*¹であることのみが規定されていて、具体的な実現手段は明確ではありませんでした。

● 日本におけるタイムスタンプの制度化

日本におけるタイムスタンプを含むタイムビジネス標準化の動きは2002年1月から6月にかけて複数回行われた総務省主催のタイムビジネス研究会から始まります。この研究会において、日本のタイムビジネスの方向性が示されました。

その後、民間主体のタイムビジネス推進協議会が2002年6月に設立されました。また、NICTは総務省から委託を受け、2003年度から2005年度にかけて「タイムスタンプ・プラットフォーム技術の研究開発」を実施しました。

さらに総務省は2004年11月に「タイムビジネスに係る指針～ネットワークの安心な利用と電子データの安全な長期保存のために～」を公表

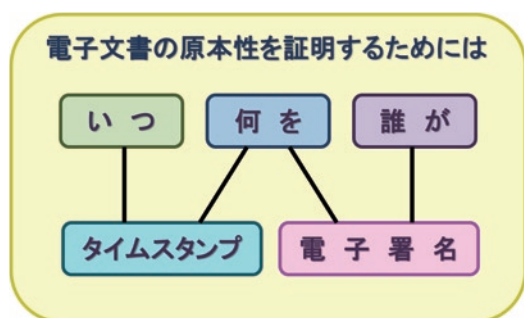


図1 電子文書の原本確保のための技術

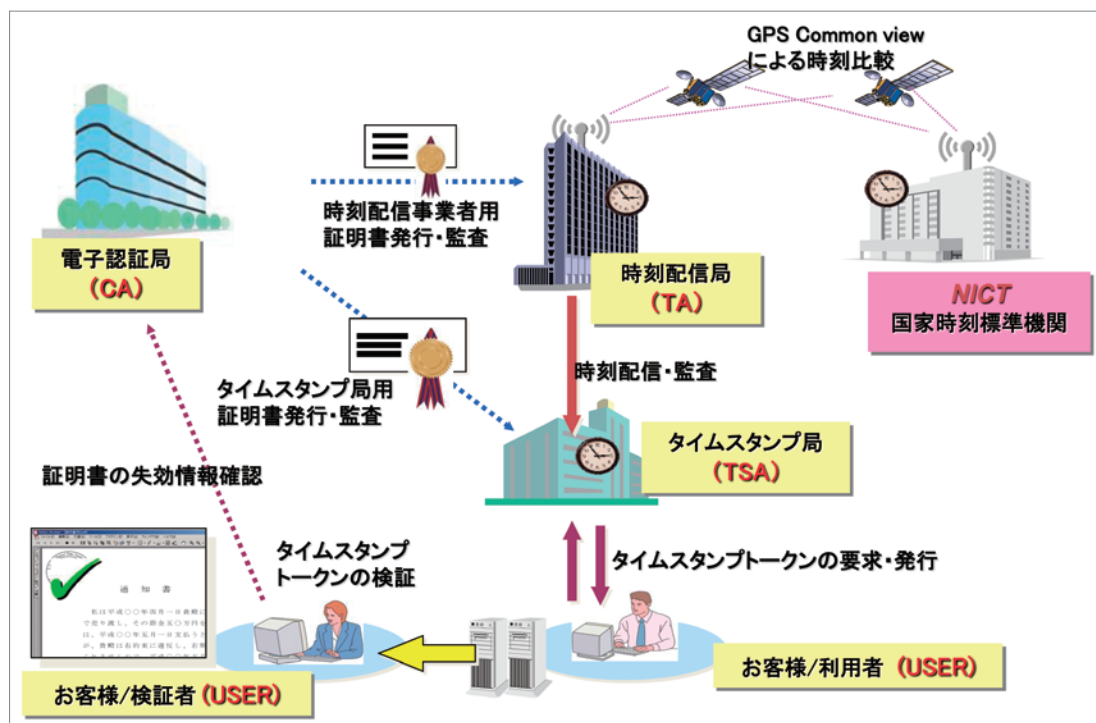


図2 日本のタイムスタンプの仕組み(デジタル署名方式の例)

しました。この指針により2005年2月から日本のタイムスタンプの仕組みを制度化した「タイムビジネス信頼・安心認定制度」が創設されたのです。

● 時刻の信頼性を重視した日本のタイムスタンプ制度

日本のタイムスタンプ認定制度における特徴は、タイムスタンプの根幹となる時刻の信頼性に重きを置いた点です。これまでタイムスタンプに用いる時刻についてはUTCへのトレーサビリティは求められるものの時刻の正確さについての規定はありませんでした。

日本の認定制度では、NICTの標準時と同期した時刻をタイムスタンプ局 (Time Stamping Authority: TSA) などに配信し、かつ、TSAがタイムスタンプに用いる時刻の正確さを監査する第三者機関として、時刻配信局 (Time Authority: TA) を規定しました。これにより、日本のタイムスタンプ制度においてはTSAの信頼できる時刻源の仕組みが明確化されました (図2)。

● ITUにおける勧告化^{*2}への道のり

NICTは日本の標準時に責任を持つ機関として、2000年の国際電気通信連合 科学業務に関する研究委員会 標準時及び標準周波数の通報に関する作業部会 (ITU-R SG7 WP7A) 会合に、タイムスタンプ局が用いる時刻の信頼性をいかにして確保するかを日本からの研究課題として提案しました。この研究課題は、修正のうえITU-R 238/7として採択されました。

2009年9月のITU-R SG7 WP7A会合において前述の日本で実際に制度化されているタイムスタンプ制度の仕組みをNICTが取りまとめ、国内委員会の承認を得たうえで日本からの勧告案として提出しました。提出された勧告案は時機を得た提案として各国から好意的に受け

入れられ、表現の修正などはありませんでしたが、ほぼ日本提案がそのままSG7に送られました。その後、2010年1月にSG7により採択され、この採択を受けITU-Rは直ちに承認手続きに入り、2010年4月に勧告案は勧告ITU-R TF.1876として承認されました。今回の勧告は提案からわずか7カ月という異例の速さで勧告化されたわけです。

● 勧告 ITU-R TF.1876の概要

今回の勧告の主旨は次の4点です。

- ・各国の時刻標準機関は要求される正確さでTSAに各機関のUTC (UTC (k)) を供給しなければならない。
- ・TSAからUTC (k) への時刻のトレーサビリティはタイムアセスメント機関 (Time Assessment Authority: TAA) による連続的なモニタリングで証明されなければならない。
- ・TAAはTSAの用いる時刻が要求される正確さを維持しているかどうか監査する機能も有する。
- ・TAAは各国の時刻標準機関または信頼できる第三者機関が行うべき機能である。

この勧告でTAAという機能を定義付けました。TAAはこれまでのTAを包含する機能であり、より一般化した概念です。ただし、この勧告はTAAという機能について定義しただけですので、今後の補強も求められています。このTAAの概念を導入することにより、日本のタイムスタンプの仕組みを海外に輸出する下地ができました。日本の認定制度においてもTAの機能がTAAに変更になりました (図3)。

● さらなる標準化への動き

このようにITUで勧告化された日本のタイムスタンプの仕組みですが、海外に輸出するためにはさらなる標準化が必要になります。

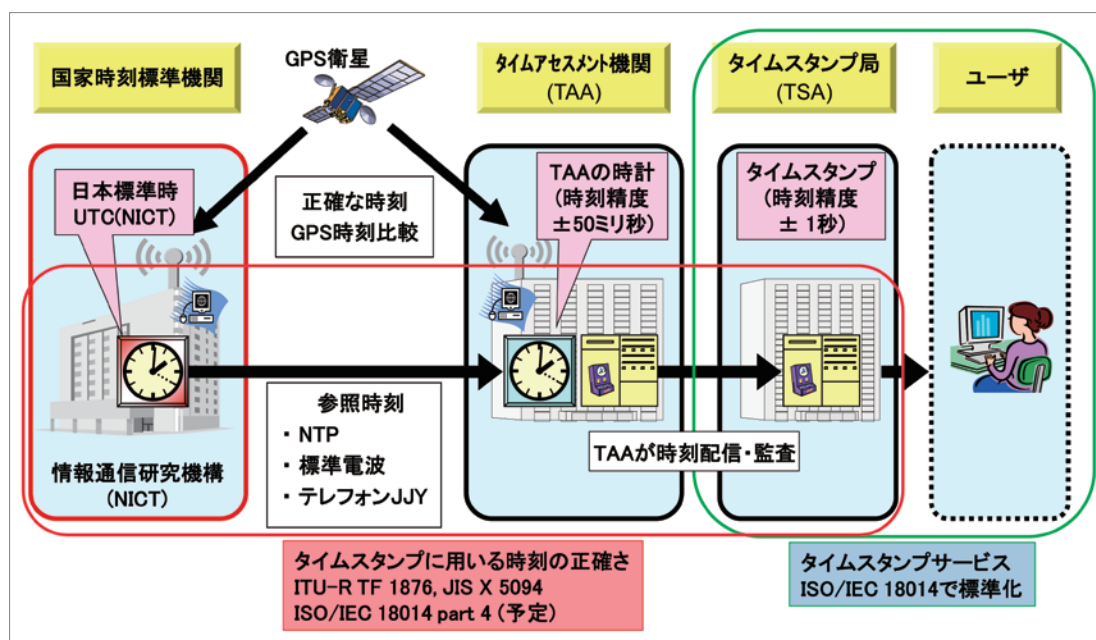


図3 日本のタイムスタンプの仕組みの標準化状況

まず日本の認定制度の運用実績をもとに、ITU-R勧告に認定制度の技術基準の数値を付加して日本工業規格 (JIS) として標準化作業を行い、2011年5月に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」として制定しました。

このJIS X 5094をもとに国際標準化機構 (ISO) において標準化作業に着手しました。

ISOの国内委員会の審査を経てISO/IEC 18014のpart4として2011年6月に作業文書 (WD) を提出、10月のSC27WG2会議の審議を経て、各国からの意見に対処して修正し2012年5月には委員会文書 (CD) に昇格しています。このように現在JISで制定した日本の標準を、ISO/IECの国際標準にするための作業の最中です。

タイムスタンプの付与技術についてはISO/IEC 18014として標準化されていますが、時刻を保証できるシステムとして整備されている国はまだほとんどありません。日本のタイムスタンプの仕組みは世界的にも評価されており、ITUにおける勧告化を足がかりに日本のタイムスタンプ

の仕組みを同じISO/IEC 18014のpart4として世界の標準にするよう今後とも取り組んでいきます。

用語解説

*1 トレーサブル

タイムスタンプで用いる時刻が、正確さと不確かさ込みで UTC までさかのぼることができること。

*2 ITU 勧告について

ITU では、電気通信や放送技術に関わるさまざまな国際的な決まりを作っています。ITU-R 勧告は、主に ITU-R SG の研究活動の成果として策定され、ITU メンバーステートによって承認された国際技術基準で、分野別にシリーズ化し、番号が付されます。