2-6　日本のタイムビジネスの動向

2-6 Trend of Time Business in Japan

岩間　司　　齊藤春夫　　町澤朗彦　　鳥山裕史
IWAMA Tsukasa, SAITO Haruo, MACHIZAWA Akihiko, and TORIYAMA Hiroshi

要旨

日本のタイムビジネスは、2002年1月に総務省で開催されたタイムビジネス研究会から始まり、NICTは日本の国家時刻標準機関としてタイムビジネスの黎明期から深く関わってきた。本稿ではタイムビジネス協議会とタイムビジネス認定センターを中心とした日本におけるタイムビジネスの動向と、「タイムスタンプ・プラットフォーム技術の研究開発」をはじめ、これまでNICTが行ってきた研究開発及び標準化活動についてまとめる。

Time Business in Japan started from the report of Ministry of Internal Affairs and Telecommunications of January, 2002. NICT participated in Time business from the beginning. In this paper, we describe the trend of Time business in Japan, research and development and standardization activity of NICT.

[キーワード]
タイムビジネス，タイムスタンプ，タイムビジネス信頼・安心認定制度，国際電気通信連合
Time business, Time stamping, Accreditation program for time-stamping services, International Telecommunications Union (ITU)

1　まえがき

日本のタイムビジネスは、2002年1月の総務省で開催された「標準時配信・時刻認証サービスの研究開発に関する研究会（通称：タイムビジネス研究会）」から始まった。タイムビジネス研究会は、2002年1月から6月までの期間に5回開催され、日本のタイムビジネスの将来イメージやその実現方法が示された[1]。

この研究会を受けて産学官協調のタイムビジネス推進協議会が2002年6月に設立された。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」を実施した[2][3]。これらの研究成果から総務省は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～」[4]を公表した。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。タイムビジネス推進協議会は、タイムビジネス立ち上げのためのガイドラインや制度等を一通りまとめ上げて2006年6月に活動を終了した。そしてより普及・啓蒙に尽力しタイムビジネスの発展を図る目的でタイムビジネス協議会が設立され現在に至る。

NICTは直接利用者との接点は持たないが、日本の国家時刻標準機関としてタイムビジネスの黎明期から深く関わってきた。NICTの活動の場は主として総務省の政策と深く関わる場合や国際電気通信連合（International Telecommunications Union：ITU）の場である。NICTが総務省の政策に関わった主な活動として前述の「タイムスタンプ・プラットフォーム技術の研究開発」がある。この活動は単に総務省の指針や「タイムビジネス信頼・安心認定制度」の策定のみならず、現行のサービスや企業間の連携といった実際のタイムビジネスの基盤作成に大いに役立つこととなった。

ITUに関わる活動では2000年のITU-R SG7 WP7A会合に、タイムスタンプ局が用いる時刻の

図1 電子文書のハッシュ化

信頼性を如何にして確保するかについて研究することを日本からの研究課題として提案したことから始まる。この研究課題は修正のうえ「研究課題 ITU-R 238/7 タイムスタンプ局の信頼できる時刻源(Question ITU-R 238/7 Trusted Time Source for Time Stamp Authority)」として採択された。そして2009年9月のITU-R SG7 WP7A会合において上記の日本型のタイムスタンプ制度について勧告案を提出し、提出された勧告案は、表現の修正などの後SG7に送られた。9月のSG7会合ではSG7に参加している全メンバーステートに対し文書による採択手続きを行うことを決定し、2010年1月にSG7により採択された。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として承認された。

NICTがITUに研究課題を提出してから10年、またタイムビジネス研究会から8年余が過ぎ日本のタイムビジネスは事業として日本の社会にしっかりと根を張り始めた。本稿では日本のタイムビジネスのこれまでの10年と今後の方向性について検討する。

2 タイムスタンプの仕組み

2.1 電子文書における脅威

タイムビジネスについて述べる前にタイムビジネスの中心的な技術であるタイムスタンプの仕組みについてまとめる。

パソコンなどを使って作成する電子文書及びスキャナなどで紙文書を電子化した電子化文書は、何回複製(コピー)しても劣化の心配がなく、対応するソフトウエ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ある(以降、特段の必要がない限り電子文書と電子化文書を総合して電子文書という)。この利点は逆に、元の電子文書を改ざんしたり、他人になりすまして電子文書を作成することも容易にできてしまうことになる。これら文書の「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る。

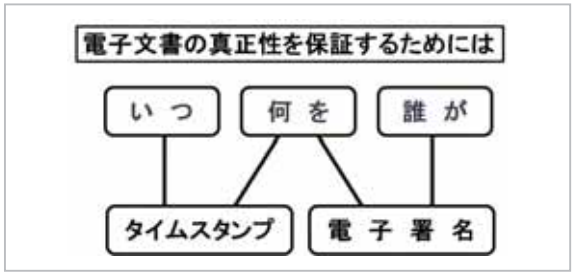

図2 電子文書の真正性

これら電子文書の「改ざん」や「なりすまし」を防ぐために有効な手段としては電子署名やタイムスタンプがある。

2.2 電子署名とタイムスタンプ

電子署名とタイムスタンプは、暗号技術を用いて電子文書の原本性を証明する技術の1つであり、日本のみならず海外でも利用されている。

電子署名では、図1に示すように最初に任意の電子文書を一方向ハッシュ関数によって一定の長さの固定データ(ハッシュ値)に変換する。この変換されたハッシュ値をメッセージダイジェストと言う。生成されたメッセージダイジェストをさらに電子文書の作成者自身の秘密鍵で暗号化する。この作成者の秘密鍵による暗号化を署名行為と言いここで生成された暗号化されたメッセージダイジェストが電子署名である。

メッセージダイジェストの生成過程や暗号化に安全性が証明された暗号技術を用いることにより、図2に示すように電子署名によって「誰が」「何を」作成したかを証明することができる。

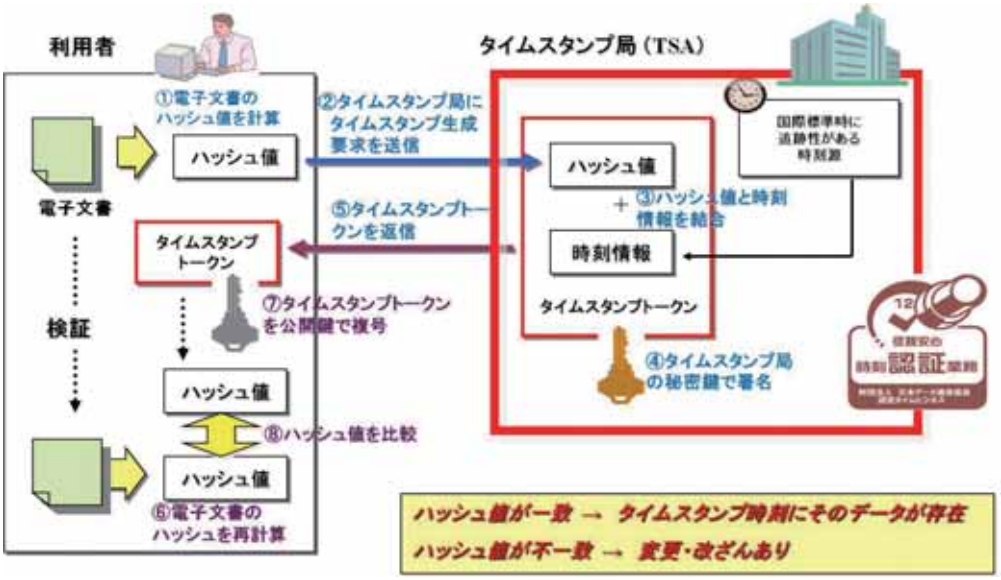

図３　タイムスタンプの仕組み

一方タイムスタンプでは、最初に任意の電子文書のメッセージダイジェストを生成するところは同じであるが、タイムスタンプを生成するためにはこのメッセージダイジェストをタイムスタンプ局（Time Stamping Authority：TSA）に送る。TSAでは、このメッセージダイジェストに時刻情報を付加してタイムスタンプを発行する。そしてタイムスタンプでは電子署名と同様に、「何を」作成したかを証明することができる。またタイムスタンプでは電子署名と異なり「誰が」の代わりに「いつ」作成したかを証明できる。この一連の仕組みについて図３に示す。

これら電子署名とタイムスタンプを併用することにより図２に示すように「いつ」「誰が」「何を」作成したか証明できることになる。これが電子文書の「真正性」すなわち「文書の作成者・作成時期、作成された電子文書または紙文書などと電子化した文書が同一であり改ざんされていない」ことを保証することになる。

このように電子署名／タイムスタンプ技術では暗号技術に基づいて電子文書の安全性を保証している。逆にいうと、暗号技術に何らかの脆弱性が生じたときは大きな影響を受けることになる。この影響についての実例は、「タイムビジネス認定センター」の項で詳しく述べる。

3　タイムビジネスの開始と普及

ここでは日本におけるタイムビジネスの始まりから現代までの変遷について、関係各団体の果たした役割を中心に述べる。

タイムビジネスのビジネス活動は、2002年から2006年までの黎明期と2006年から現在までの普及期に大きく分けることができる。

この2006年とは業界団体である「タイムビジネス推進協議会」が「タイムビジネス協議会」に引き継がれた年である。このことからこれらの団体の位置付けが理解できる。

3.1　黎明期

3.1.1　タイムビジネス研究会

黎明期における各機関の関わり合いについて図４にまとめる。

2002年以前にもすでにタイムスタンプなどのビジネスサービスは存在したが、日本における統一的なタイムビジネスの始まりは、2002年１月の総務省で開催された「標準時配信・時刻認証サービスの研究開発に関する研究会（通称：タイムビジネス研究会）」から始まった。

タイムビジネス研究会は、IT社会の実現に向け、「タイムビジネス」を考慮した情報通信基盤を

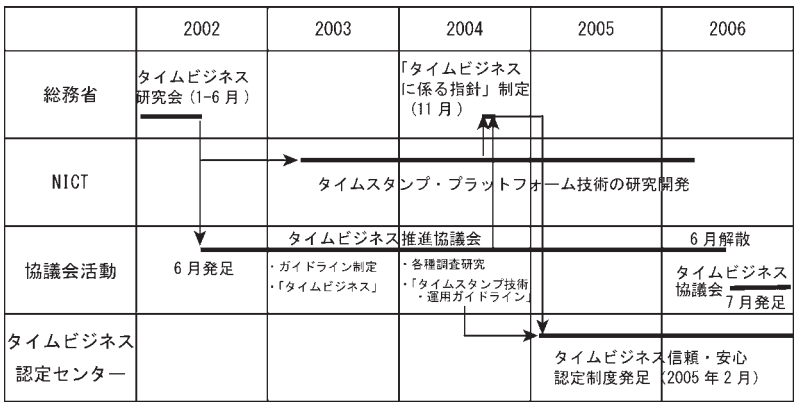

図 4　黎明期における各機関の関係

図 5　タイムビジネスの将来イメージ

（「標準時配信・時刻認証サービスの研究開発に関する研究会」報告書より）

整備するために開かれ、1 月から 6 月までの期間に計 5 回開催された。NICT からは当時の理事である塩見が委員として参加した。

研究会では

- タイムビジネスとは何か
- タイムビジネスの将来イメージ
- タイムビジネスの社会的・経済的効果
- タイムビジネスの研究開発課題・標準化課題
- タイムビジネスの総合推進方策

について積極的に議論され、報告書にまとめられた。

タイムビジネス研究会の大きな成果は、タイムビジネスを「“時刻配信”や“時刻認証”に関する業務」と位置付け、図 5 に示すようなタイムビジネス

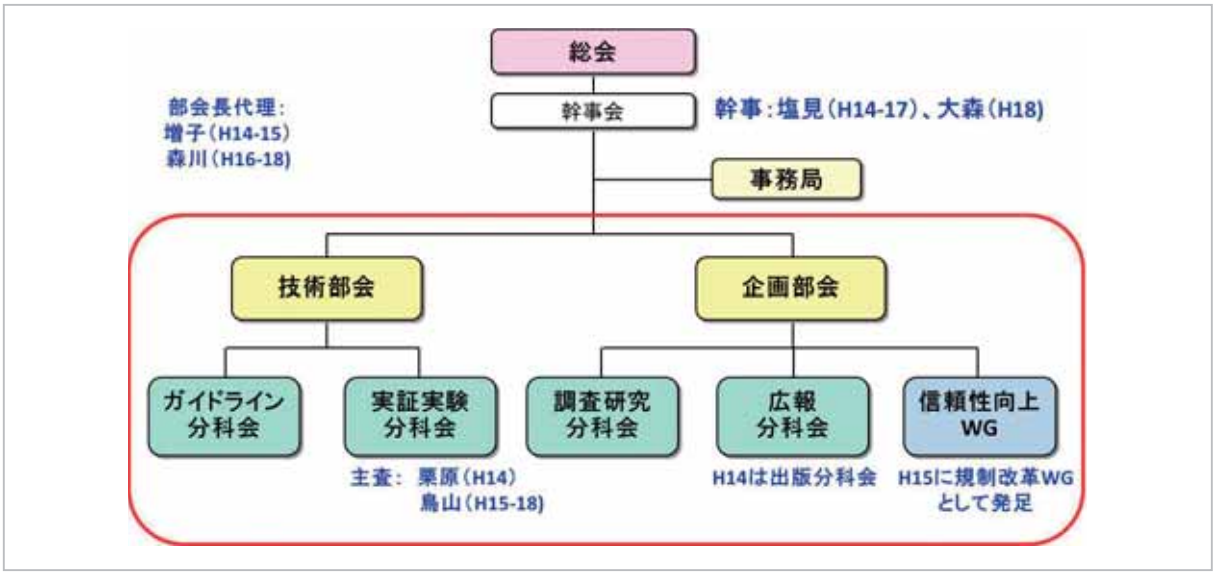

図６　タイムビジネス推進協議会組織図

の将来イメージを明確化し、実現するための手順を提示したことである。このタイムビジネス研究会でまとめられた方向性がその後の日本のタイムビジネスの在り方を決定づけた。

この時点では、タイムビジネスに“時刻配信”についても“時刻認証（タイムスタンプ）”と同等に取り扱われていたが、次第にビジネスとしての対象から時刻配信は外れていき、タイムスタンプを中心とした活動に移っていくことになる。

3.1.2　タイムビジネス推進協議会

タイムビジネス研究会で示された方向性に従って日本のタイムビジネスを実現するために、産学協調の業界団体としてタイムビジネス推進協議会（以下、「推進協議会」と省略する）が2002年6月に設立された。

推進協議会の活動母体は、図6に示すように技術部会と企画部会の2つの部会で構成され、各部会の下にそれぞれ2つの分科会が常設されていた。また、必要に応じてWGを作成して活動を行った。

NICTは、技術部会の下の実証実験分科会の主査を担当し、実証実験分科会をベースとして**4**で詳述する総務省から委託された研究開発などを実施した。

推進協議会は2006年6月までの4年間活動を行った。活動成果の主なものは以下のとおりである。

出版物
- 「タイムビジネス」（NTT出版：2003年）
- 「概説　e-文書法」（NTT出版：2005年）

ガイドライン
- 時刻認証基盤ガイドライン（2003年、2003年英語版、2004年第2版）
- e-文書法におけるタイムスタンプ運用ガイドライン（2005年）
- タイムスタンプの長期保証ガイドライン（2005年）
- 信頼される時刻認証基盤のための技術・運用基準ガイドライン（2005年）

実証実験報告書（2005年、2006年）

調査報告書
- 国内動向（2004年）
- ドイツ（2004年）
- 国内及び海外（2005年）
- 英国、ハンガリー、スロバキア（2006年）

これらの出版物以外の報告書は現在でもタイムビジネス協議会のWebページから入手できる[5]。

特に「時刻認証基盤ガイドライン」の作成は推進協議会が最初に取り掛かった作業で、日本のタイムビジネスの形態を具体化した最初のモデルであ

る。ここで時刻配信の大本にNICT（当時はCRL）を配置したことにより、日本のタイムビジネスではNICTを国家時刻標準機関として位置付けることとなった。

実証実験報告書は、NICTが中心となって実施した「タイムスタンプ・プラットフォーム技術の研究開発」の結果を他の会員の目を通じて評価した結果を求めたものである。

この実証実験の結果を含め、「時刻認証基盤ガイドライン」及び国内外の調査報告書の成果をもとに、総務省は2004年11月「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～」[4]を公表した。

この「タイムビジネスに係る指針」をもとに、「信頼される時刻認証基盤のための技術・運用基準ガイドライン」を参考に技術基準及び運用基準を定めて「タイムビジネス信頼・安心認定制度」が発足した。

推進協議会期間中のもう1つの大きなエポックは、2004年11月に「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（通則法）及び「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（整備法）として成立し、2005年4月から施行された通称「e-文書法」である[5]。

「e-文書法」とは、民間企業が作成・保存を義務付けられている文書・帳票類の電子化を可能とするための法律である。

e-文書法における電子化文書においては「真正性」を保証することが必要となる。この真正性を保証する技術として**2**で述べたように、電子署名とタイムスタンプの組み合わせが利用できる。

この「e-文書法」におけるタイムスタンプの利用について、推進協議会を挙げて関係省庁に積極的に働きかけを行った。その結果、「e-文書法」において国税関連文書、地方税関連文書及び医療関連書類など、保存が義務付けられた文書の一部について電子署名及びタイムスタンプを用いた電子化保存が可能となった。

このように推進協議会は「タイムビジネス信頼・安心認定制度」の発足や「e-文書法」対応などに大きな足跡を残しつつ、タイムビジネスの立ち上げと初期の普及・啓蒙に多大な貢献を果たして2006年6月に活動を終了した。翌月から新たにタイムビジネス協議会が設立されて普及期に入る。

3.2 普及期

3.2.1 タイムビジネス認定センター

「e-文書法」でタイムスタンプを用いることにより電子化文書の保存が可能となったが、ここで用いるタイムスタンプはなんでも良いわけではない。e-文書法（整備法）に基づき個別に定められたe-文書法の個別法のうち国税関連帳簿類や医療分野に係る書類に関する省令等[6]では「財団法人日本データ通信協会が認定する業務に係るタイムスタンプ」を使用することになっている。

この民間によるタイムスタンプの認定制度が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の運用する「タイムビジネス信頼・安心認定制度」である。

「タイムビジネス信頼・安心認定制度」は前述の通り黎明期の終盤、2005年2月に発足した。認定制度の組織形態として、審査の公正を保つため、学識経験者を中心に構成されている制度諮問委員会（制度の評価や見直しの検討）と認定審査会（当協会だけで判断困難な申請案件の審査）を設置している。これらの委員会にNICTのメンバーも委員として選任されている。

認定基準は以下の観点に基づいて審査を行う。

- 技術基準
- 運用基準
- ファシリティの基準
- システム安全性の基準
- サービス加入者及びサービス加入者に関わる関係社への説明事項

ここで技術基準及び運用基準は前節の推進協議会で作成した「信頼される時刻認証基盤のための技術・運用基準ガイドライン」をベースに、より実用的に改善した基準を用いている。本来ならばこれらの基準はすべて根拠となる規格を有するべきである。しかしながら、例えばTSAのポリシ要件についてはRFC3628、タイムスタンプの付与についてはISO/IEC17025など、個別の要件については国際的な規格があるが、時刻の配信／監査については国際的な規格が定められていない。これについては**4**で述べるが現在、NICTが中心となって国内／国外で標準規格の整備を進めている。

また**2**で述べたようにタイムスタンプ技術は暗号技術に基づいて安全性の保証を行っているため、暗号技術の脆弱性は、そのまま認定制度の脆弱性に結び付く可能性がある。認定制度が開始された2005年から2010年度までに暗号の脆弱性に伴い2回の対応検討が行われた。

1回目は認定制度発足直後の2005年10月から2006年1月にかけて「SHA-1の衝突困難性の脆弱化」の問題に対して対策を検討した。その結果、2006年4月以降、電子文書をハッシュ化する際には「SHA-256以上のビット長を持つハッシュ関数を使用すること」が追加された。

2回目の脆弱化は執筆を行っている2010年時点に現在進行形で検討されている「SHA-1及びRSA1024暗号アルゴリズムの脆弱化」の問題である。これらの脆弱性について電子署名などについては内閣官房セキュリティセンターなどでは2014年度末までの生成終了を目標とした移行スケジュールを策定中であるが、タイムスタンプでは1年前倒しした2013年度末を目途とした移行スケジュールを策定し、移行準備を進めているところである。

「タイムビジネス信頼・安心認定制度」は民間の認定制度でありながら系統的に整備されたタイムスタンプの認定制度として現在のタイムビジネスの中心となる制度である。

3.2.2 タイムビジネス協議会（Time Business Forum： TBF）

タイムビジネス協議会（以下、「TBF」と省略する）は、推進協議会の解散後、推進協議会の成果を引き継ぎ、より使いやすく信頼されるタイムビジネスの展開を図り、広く社会への普及・浸透を促す取組みを目指して2006年7月に設立された。

組織の在り方としては図7(a)の当初の組織構成からわかるように利活用領域に関する検討にウエイトがかかり、より実用的な普及を目指していることがわかる。

これについては、2005年4月のe-文書法の他

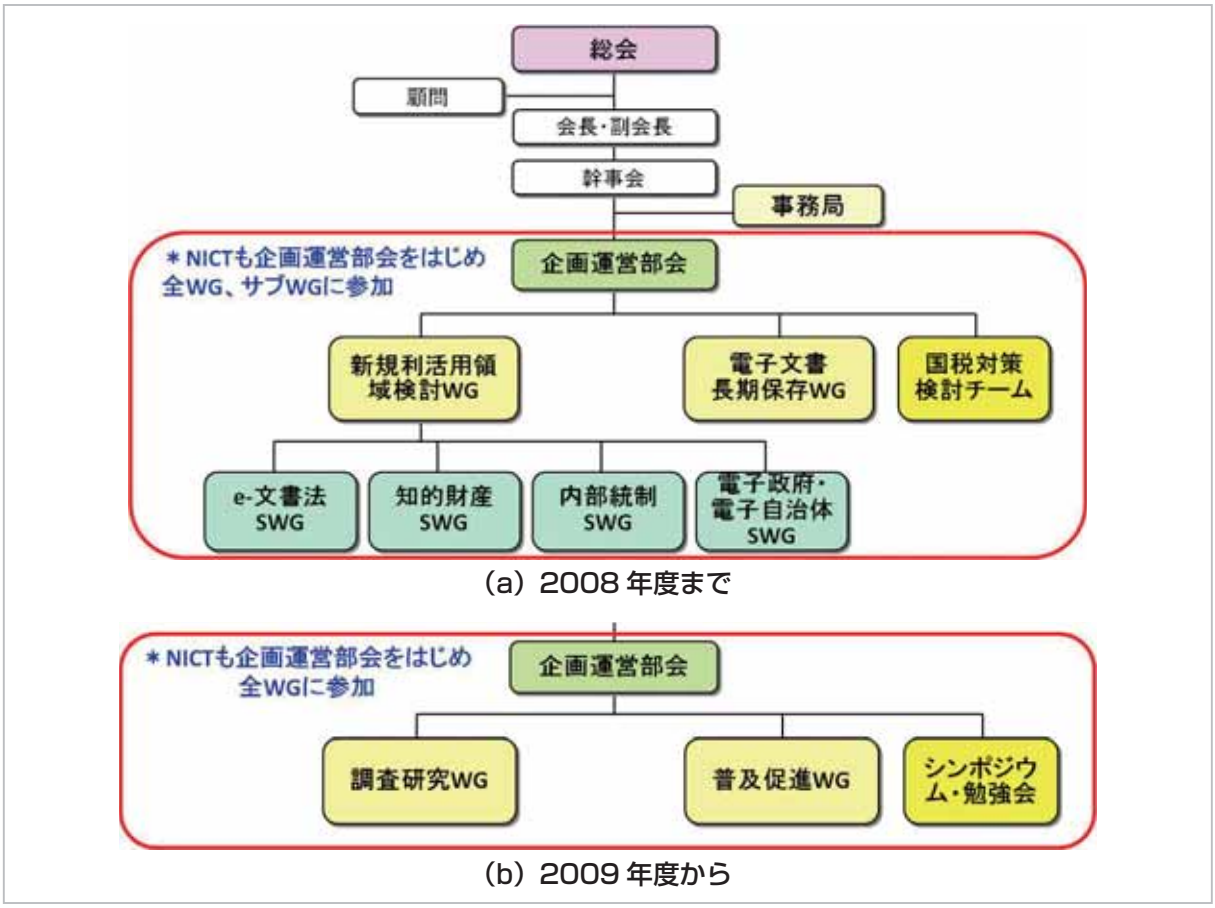

図7 タイムビジネス協議会組織図

にも 2005 年 3 月の厚生労働省による「医療情報システムの安全管理に関するガイドライン」や 2006 年 6 月の特許庁による『先使用権制度ガイドライン（事例集）「先使用権制度の円滑な活用に向けて－戦略的なノウハウ管理のために－」について』[6] など各省庁が主導する電子化の流れの中にタイムスタンプが盛り込まれているからである。

しかしながら、タイムスタンプの普及には、これら各省庁の制定するガイドラインだけではなく、TBF を中心した各企業の普及への努力があった。例えば、2006 年の「e-文書法サブワーキンググループ 2006 年度報告」にあるように、市場調査の結果を分析し、それを基に方針を立てて普及を図るという方法を採用した。また、これまでの提供者を対象としたガイドラインだけではなく、2007 年に作成した「知的財産におけるタイムスタンプ活用ガイド」のようにポンチ絵を多用し、利用者にも分かり易い小冊子を作成した。これらの対策により、実際の普及が図られてきたわけである。

これらの対策により、2008 年後半のいわゆるリーマンショックによる景気の冷え込みがあったにもかかわらず、2008 年以降にタイムスタンプの利用を開始した企業が増加していることが 2010 年に掲載された「タイムスタンプ活用事例」[7] に表れている。

推進協議会から TBF になり、NICT との関係も変化した。推進協議会の時は、部会長代理や分科会主査を務め、また総務省との関係から運営に近い立場だった。しかし、TBF になってからは、より民に近い組織となり、NICT も一参加団体として活動を行っている。

それでも 2007 年度から 2008 年度にかけてクライアント側時刻認証システム実現のために“Managed Time-stamping Service（MTS）”の実現可能性について TBF に研究提案を行い、WG で共同で検討を行い、タイムビジネス認定センターへ提案を行うなど共同での活動も実施してきた。

TBF は、TBF の活動がそのまま各企業間の利益活動に結び付きにくいところもあり、近年の景気の停滞により、2010 年度には、大幅な活動の見直しが行われている。組織活動の意義は、参加企業全体が認めているので 2011 年度にはよりスリム化した組織となって再始動する予定である。

4 NICTの活動

4.1 総務省委託研究

タイムビジネス研究会で示された方向性、及び総合科学技術会議の「平成 15 年度の科学技術に関する予算、人材等の資源配分の方針」の重点 4 分野の 1 つである情報通信分野において、情報通信システムの安全性・信頼性確保の必要性が特に言及されていることなどを受け、安全性・信頼性確保に貢献する研究開発として 2003 年春、「タイムスタンプ・プラットフォーム技術の研究開発」が総務省より NICT に委託され、タイムアプリケーショングループを中心として研究開発を行った。

本研究開発では、「タイムスタンプ・プラットフォーム技術」を確立するために以下に示す 3 つの技術課題を掲げシステム開発を実施した。

- 高精度時刻配信技術の研究開発
- 高信頼時刻認証技術の研究開発
- 高速時刻認証技術の研究開発

本システム開発では単独の要素技術ではなく、各機能相互の連携が重要であるため、図 8 に示すタイムスタンプ・プラットフォームシステムを開発して機能確認を行った。

また情報セキュリティに関する様々な問題に対して開発したシステムの安全性を評価するため、タイムスタンプ用のセキュリティ・ガイドラインを制定し、タイムスタンプ・プラットフォームシステム全体のセキュリティ評価を実施した。

それぞれの研究成果について簡単にまとめる。

4.1.1 高精度時刻配信技術の研究開発

タイムスタンプ・プラットフォームシステムでは、4.1.2 の高信頼時刻認証技術の研究開発で策定された時刻認証プロトコルの違いにより、図 8 の国家時刻標準機関 NTA1、時刻配信局 TA1、タイムスタンプ局 TSA1 及び TSA2 からなる「認証連鎖方式」と国家時刻標準機関 NTA2、時刻配信局 TA2 及び NTP（Network Time Protocol）サーバからなる「時刻リンク方式」の 2 種類の時刻配信・認証方式がある。相手方認証や監査の方式は異なるが、どちらの方式においても時刻配信プロトコルには NTP を使用している。

認証連鎖方式のシステムでは、NTA1 を東京都小金井市、TA1 及び TSA2 を千葉県千葉市（幕張）、TSA1 を中央区築地に配置してそれぞれの

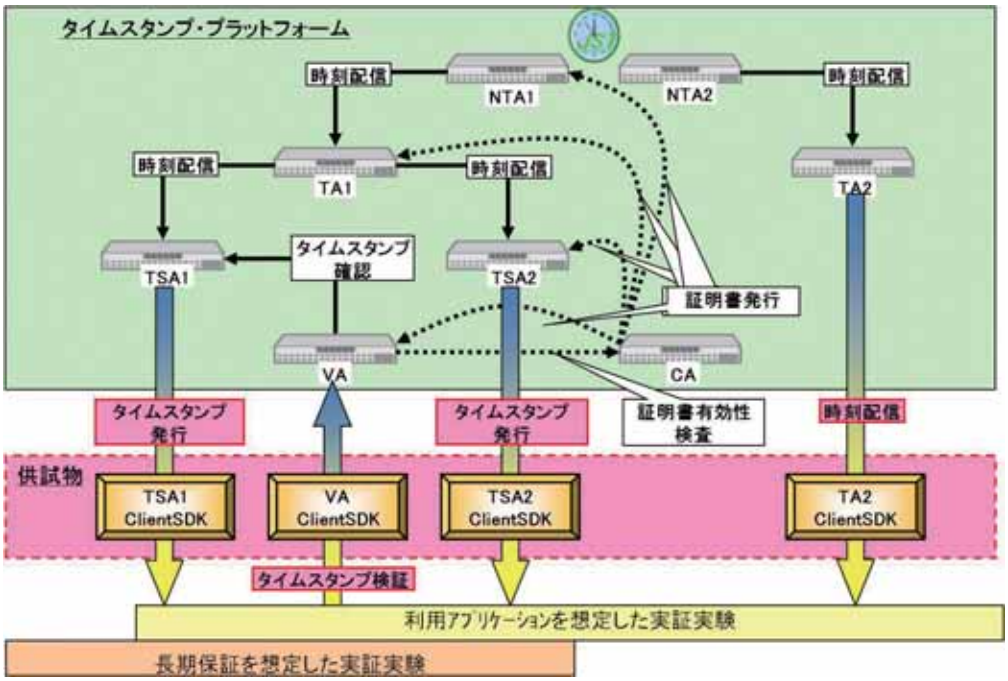

図８　タイムスタンプ・プラットフォームシステム構成図

局間を ISDN 64 kbps で接続した。NTA1/TA1 間の時刻配信において 1 週間の測定期間内で時刻誤差が± 1 ミリ秒を超えた割合は約 4 %あったが、散発的な発生で使用機器内の割り込み処理によるものと考えられる。また NTA1 から TSA1、TSA2 までの時刻配信において± 10 ミリ秒を超えることはなかった。

時刻リンク方式のシステムでは、NTA2 及び TA2 を東京都小金井市、NTP サーバを港区新橋に設置して局間を 10 Mbps で上り下り対称なインターネット回線で接続した。こちらはインターネット回線を用いているため、トラヒックの影響を受けるが、ほぼ 1 ミリ秒以内を達成している。また、ローカルに直接 10 Mbps で接続した場合でも 1 ミリ秒を超える場合があり、主として割り込み処理によるものであった。また NTA2 から NTP サーバ間の時刻誤差はやはり± 10 ミリ秒を超えることはなかった。

以上の結果から、いずれの方式においても NTA から TSA までの時刻誤差は± 10 ミリ秒を超えることはなかった。また、時刻精度劣化の要因は、測定結果からネットワーク上の不要なトラヒックによるものと装置内での他のプログラムによる割り込み処理が主たる要因であると考えられる。

4.1.2　高信頼時刻認証技術の研究開発

タイムスタンプ・プラットフォームシステムでは、時刻認証プロトコルの違いにより「認証連鎖方式」と「時刻リンク方式」の 2 種類の時刻配信・認証方式を採用した。「認証連鎖方式」では TSA1 でリンク情報を用いるアーカイビング方式タイムスタンプを、TSA2 で PKI 方式タイムスタンプをそれぞれ発行している。PKI 方式タイムスタンプでは、各局における時刻情報を含んだ時刻監査証明書をタイムスタンプトークンに順次付与することにより、配信経路と時刻誤差を検証時に確認できる。また、アーカイビング方式タイムスタンプでは検証時に TSA 局の公開する時刻監査レポートを閲覧することにより、配信経路と時刻誤差を確認できる。

またこれらタイムスタンプの方式を意識せずにユーザがタイムスタンプ検証を行うことができる手段として、タイムスタンプ検証局（VA： Verification Authority）を新設した。VA を用いることにより、上記のタイムスタンプの方式の差異に関わらずタイムスタンプ検証時に合わせて配信経路

と時刻誤差を確認できる。

ちなみにここで開発されたアーカイビング方式タイムスタンプは現在、(株)NTT データにより認定タイムスタンプとして実用化されている。また、PKI 方式タイムスタンプで開発された時刻情報を含んだ時刻監査証明書をタイムスタンプに準じ付与する方式は(株)セイコーインスツルによって改良の上、認定時刻配信方式として実用化されている。

「時刻リンク方式」では、時刻認証に用いられる時刻認証子に時刻情報のほかに受信時の時刻誤差、生成機関情報、過去の時刻認証子ハッシュ等を含めて生成し、NTP パケット内に時刻認証子を含めて配信する。各局内では自身の局の生成する時刻認証子のハッシュと各局から送られてくる時刻認証子のハッシュを用いてハッシュリンクを生成する。このハッシュリンクは接続している各局からの時刻認証子も内包しているため、時刻認証子の改竄が行われた場合、改竄を検知することができる。「時刻リンク方式」では NTP サーバ等のログに時刻認証子を埋め込むことができ、後日、時刻認証子に含まれている情報により、改竄検知のほか時刻誤差、生成機関情報、配信経路の情報を確認できる。

この「時刻リンク方式」は、2006 年度のメール中継サーバの研究に発展したが実用化には至らなかった。

「認証連鎖方式」、「時刻リンク方式」とも、配信経路、時刻誤差などの NTA で生成された時刻であることを証明可能とするための技術が盛り込まれている。また、VA の新設により、タイムスタンプの方式の差異に関わらずタイムスタンプ検証が可能となり合わせて、検証時にタイムスタンプの有効期限が迫っている場合は、有効期限を延長する機能も有しておりユーザの利便性を高めたシステムを構築した。

4.1.3 高速時刻認証技術の研究開発

タイムスタンプ・プラットフォームシステムでは、タイムスタンプ技術としてリンク情報を用いるアーカイビング方式タイムスタンプを発行する TSA1 と PKI 方式タイムスタンプを発行する TSA2 を開発した。

TSA1 では、大量のトランザクション処理のボトルネックとなっている部分の洗い出しを行った結果、サーバ内でプロセス間通信のオーバヘッドが大きな阻害要因となっていることがわかり、この部分の改善を実施したところ最大毎秒 70,000 件のタイムスタンプ処理が可能となった。しかし、4.1.4 の「タイムスタンプ・プラットフォームのセキュリティ評価」に基づいてハッシュ関数の 2 重化、HTTPS 通信の採用などのセキュリティ改善、システム信頼化のためにタイムスタンプ発行ごとの DB 書き込み処理などの信頼性重視の処理を行うと毎秒 80 件程度のタイムスタンプ処理件数となった。本システムのセキュリティ改善及び信頼性重視の処理は安全性を重視したかなりオーバスペックな仕様となっており、かつ、安全性の処理については DB 装置の速度向上など速度改善の余地がある。

TSA2 では、大量のトランザクション処理のボトルネックとなっている部分の洗い出しを行った結果、HSM(Hardware Security Module)内部での処理速度が速度向上の阻害要因となっていることがわかった。このため、HSM 内で行っていた処理のうち 4.1.4 の「タイムスタンプ・プラットフォームのセキュリティ評価」のセキュリティ評価で問題のない部分を高速処理系で処理するようにアルゴリズムを改良したところ、最終的に 1024 ビット署名鍵を用いる場合には毎秒 130 スタンプ、タイムスタンプの安全性を高めるために 2048 ビットの署名鍵を用いる場合には毎秒 26 スタンプの処理が可能となった。さらに現在では HSM の処理性能が 10 倍以上まで向上しているため、現在市販されている HSM の性能で TSA2 の処理能力を換算すると、1024 ビット署名鍵を用いる場合には毎秒 500 スタンプ以上、タイムスタンプの安全性を高めるために 2048 ビットの署名鍵を用いる場合には毎秒 100 スタンプ以上の処理が可能となる。

これらの速度は、2010 年現在ではかなり低速に思えるが、委託研究開始当時に比べると 10 倍以上の速度改善を行ったことになる。

4.1.4 タイムスタンプ・プラットフォームのセキュリティ評価

本項目は、中間評価の時点で評価委員からの指摘に基づいて急きょ設定された研究開発項目である。

ここでは、タイムスタンプ・プラットフォームシステムをセキュリティ評価に関する国際標準 ISO/

IEC 15408 の考え方に基づいて、セキュリティ評価を実施した。NICT が策定した『統合化プラットフォーム・セキュリティ評価ガイドライン』に従い、タイムスタンプ・プラットフォームシステムのサブシステム毎の評価対象（Target of Evaluation： TOE）を明確化し、その TOE に対してセキュリティ評価を実施した。

評価の対象の主な項目は以下の 4 点である。

- 暗号コンポーネント
- 時刻情報
- 内部不正
- 将来的にタイムスタンプが検証できなくなる脅威

これらのうち、先の 2 項目は技術で対応できる項目であり、後半 2 点は運用も含めた対応が必要な項目である。

これらの評価を行った結果、4.1.3 の認証速度は低下したが安全性はより強固なシステムが構築できた。ただ、今回の評価はかなり安全性を最重要視したシステムとなっているので実際のシステム構築では、安全性と性能及び経済性のバランスを考慮すべきである。

また、このセキュリティ評価のガイドラインは現在の認定制度の審査などにも一部取り入れられている。

4.1.5 タイムスタンプ・プラットフォーム実証実験

タイムスタンプ・プラットフォームシステムを用いた実証実験において、システムを図 9 に示すように広域に配置し、様々な分野で利用されるアプリケーションを適用し、利用面から観た実用性に関する評価と技術・運用等の課題を明らかにした。さらにタイムスタンプ・プラットフォームシステムを用いた実証実験において、既に付与されたタイムスタンプの有効期間が切れる前あるいは脆弱化する前に当該タイムスタンプの効力を延長保証する技術・運用面の方策について検証を行った。

主な実験項目は次の 4 項目である。

- 電子契約実証実験
- ログサーバ実証実験
- リンク情報を使用するアーカイビング方式のタイムスタンプを用いた長期保証実証実験
- VA による長期保証実証実験

これらの実験結果は、3.1.2 で述べた推進協議会の実証実験報告書で詳細に報告しているので参照されたい。

これらの実験結果をもとに VA 以外はほとんどすべて実用化されている。また、VA の実験結果

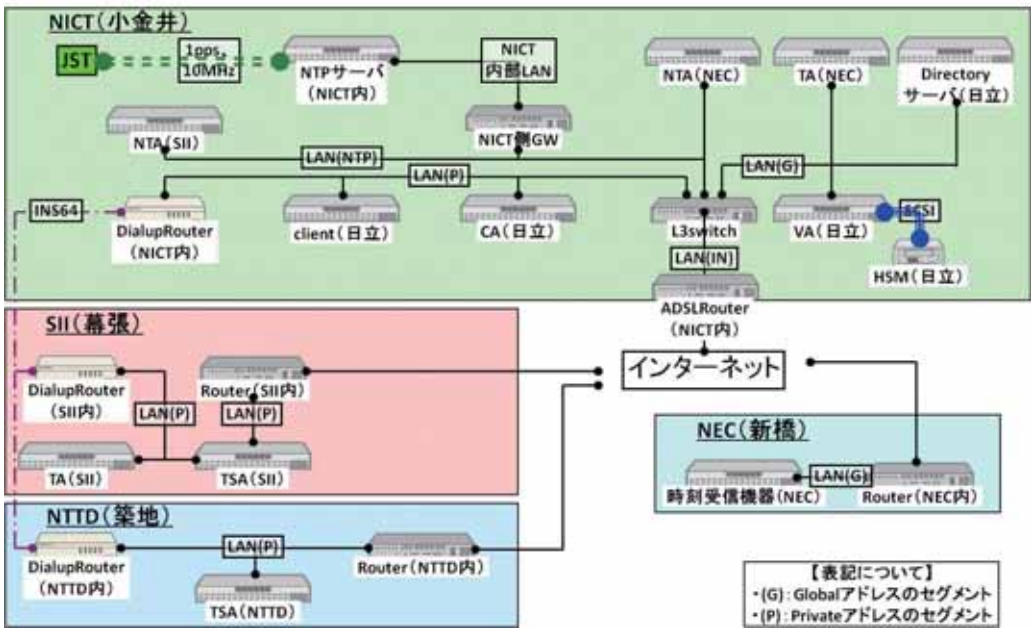

図 9 タイムスタンプ・プラットフォームシステム配置図

の延長として、様々な種類のタイムスタンプを共通に検証できる検証ツールについて、総務省はTBFに委託して検討を進めている。

タイムスタンプ・プラットフォーム技術の研究開発は、図4に示すようにタイムビジネス信頼・安心認定制度の発足に役だったのみならず、その後に実用化された要素技術も多く、日本のタイムビジネスの立ち上げに大いに貢献した。

4.2 タイムビジネスと標準化

4.2.1 国際電気通信連合における標準化

NICT（当時はCRL）がタイムスタンプに関する標準化のための研究課題を国際電気通信連合（International Telecommunication Union：ITU）に提案したのは、タイムビジネス研究会より早い2000年9月のITU-R SG7 WP7A会合である。ここでITU-Rは国際電気通信連合の無線通信部門、SG7（Study Group 7：科学業務に関する研究委員会）WP7A（Working Party 7A：標準時及び標準周波数の通報に関する作業部会）である。

タイムスタンプの付与及び検証についてはこれまで述べてきたように暗号技術を用いているため、IETF（Internet Engineering Task Force）のRFC（Request For Comment）などのようなインターネット業界で標準化がされており、その一部は国際標準化機構（International Organization for Standardization：ISO）、日本工業規格（Japanese Industrial Standards：JIS）による標準が制定されている。しかしながら、タイムスタンプのもう1つ重要なファクタであるタイムスタンプ時刻の信頼性については明確な基準が制定されていなかった。

そこで、2000年の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如何にして確保するかについて研究することを日本からの研究課題（Question）として提案した。研究課題は修正のうえ採択され「研究課題ITU-R 238/7 タイムスタンプ局の信頼できる時刻源（Question ITU-R 238/7 Trusted Time Source for Time Stamp Authority）」として研究されることとなった。

その後、2002年9月のITU-R SG7 WP7A会合ではタイムビジネス研究会で検討した国家時刻標準機関であるNICTからの時刻を基準とした日本におけるタイムスタンプサービスの在り方について報告した。参加各国、特に欧州の各国からは強い関心を得たが、その後、他の参加各国からの報告などはなかった。

通常、ITU-Rでは約4年ごとに研究課題などの見直しがあり、この研究課題についても2003年及び2007年に見直しの機会があったが、幸いにも欧州の複数の国から研究継続の提案があり継続された。

2009年9月のITU-R SG7 WP7A会合において図10に示すような日本の時刻配信局（TA）が時刻の配信と監査に責任を持つ仕組みについて勧告案を提出した。提出された勧告案は時期を得た勧告案として各国から好意的に受け入れられ、TAをタイムアセスメント機関にするなどの表現の修正などはあったがほぼ日本提案がそのままSG7に送られ、その後、SG7の採択とITU-Rの承認手続きを経て、2010年4月に勧告ITU-R TF. 1876として承認された[8]。

今回の勧告の本論は次の4点である。

- 各国の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。

ここでTAAという機能を定義付けた。これはこれまでTAとして定義付けられてきた機関を包含する機能であり、より一般化した概念である。このTAAの概念を導入することにより、日本式の時刻が正確なタイムスタンプ方式を海外に輸出する下地ができた。もちろん、この勧告はまだTAAという機能について定義しただけであるので、この勧告では今後の補強も求められている。

4.2.2 標準規格化

ITU-RにおけるTAA機能の標準化と並行し

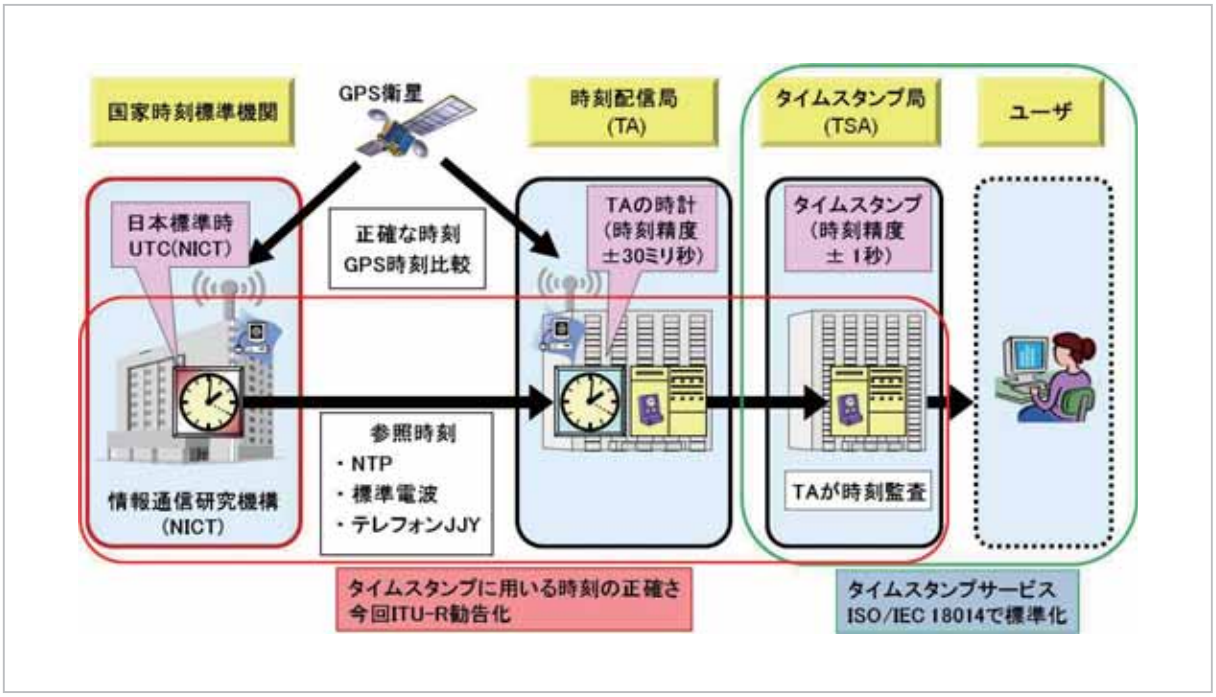

図 10　勧告 ITU-R TF.1876 の適用範囲

て、NICT では 2009 年度から「タイムビジネス信頼・安心認定制度」を運用する日本データ通信協会と共同で TAA に関する技術要件を日本工業規格（JIS）として制定する作業を開始した。

ITU-R の勧告では国際化を念頭に置いているため、TSA は TAA から供給される時刻を使用する必要はない。しかし、日本の認定制度では TSA は TAA が供給する時刻を使用することを義務付けているため、日本の認定制度に沿った標準規格を制定する必要がある。また、JIS の中に注記としてではあるが、NICT を日本の標準時を供給する機関として位置付けている。

JIS 制定の作業は実際の原案作成を行う JIS 原案作成作業班により、JIS 原案が作成され、その原案を有識者による JIS 原案作成委員会に諮って JIS 原案として申請することを決定した。そして、2009 年度末には、JIS 原案を作成して JIS を主管する経済産業省に工業標準化法第 12 号案件として JIS 化の申請を行った。

JIS 制定作業は、2010 年 8 月末に企画調整分科会によるヒアリングが行われ、委員からのコメントに基づく修正が行われ、再提出しているところであるが、2010 年 9 月現在では大きな問題の指摘はなく近く JIS として標準規格化される見込みである。

さらに日本のタイムスタンプの仕組みを海外に供給するためには国際的な標準規格化が必要となる。このため、現在の JIS 原案を基に ISO 化する作業も 2010 年度後半から開始している。

5　おわりに

タイムビジネスは、開始からまだ 10 年弱の非常に新しい分野である。しかし、高度情報通信社会の進展とネットワーク環境の急速な発展により、現代社会にはなくてはならない存在となりつつある。NICT は、日本の標準時に責任を持つ機関としてタイムビジネスの黎明期から深い関わりを持ちその発展に寄与してきた。

近年の情報漏えい事件や改ざん事件など電子文書の安全性の問題が急浮上している。加えてネットワークのクラウド化により、電子情報のセキュリティをどのようにして守るかが大きな課題となる。このような社会情勢から、この分野は国内、国外を問わず今後ますます発展していくことが予測される。その際に NICT が日本の国家時刻標準機関として、その責務を果たしていけるよう今後とも努力していく必要がある。

参考文献

1 総務省，“タイムビジネスの普及に向けて 「標準時配信・時刻認証サービスの研究開発に関する研究会」～タイムビジネス研究会～報告書，”2002 年 6 月.
2 タイムビジネス推進協議会，“タイムスタンプに関する実証実験報告書，”2005 年 5 月.
3 タイムビジネス推進協議会，“タイムスタンプに関する実証実験報告書，”2006 年 5 月.
4 総務省，“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～，”2004 年 11 月. http://www.dekyo.or.jp/tb/summary/data/MICguideline041105.pdf
5 タイムビジネス推進協議会の成果物は以下から入手可能. http://www.dekyo.or.jp/tbf/se ka/
6 タイムスタンプの利用に言及している省令及びガイドライン等は以下から入手可能. http://www.dekyo.or.jp/tb/linkdocument/index.html
7 タイムビジネス研究会，“タイムスタンプ活用事例，”日本データ通信，No. 176，pp. 11–25，2010 年 11 月.
8 ITU-R Recommendation TF. 1876，“Trusted Time Source for Time Stamp Authority，”2010 年 4 月.

岩間 司（いわま つかさ）
新世代ネットワーク研究センター
光・時空標準グループ研究マネージャー 博士（工学）
電子時刻認証技術、時刻配信応用技術

齊藤春夫（さいとう はるお）
新世代ネットワーク研究センター
光・時空標準グループ主幹
時間・周波数計測

町澤朗彦（まちざわ あきひこ）
情報推進室情報システムチームチームリーダー
画像符号化、視覚情報処理、ネットワーク計測、時刻同期

鳥山裕史（とりやま ひろし）
情報推進室室長 工学博士
情報理論、ネットワーク応用技術、電子時刻認証技術