タイムビジネスからトラストサービスへ

Evolution from Time Business to Trust Services

宮崎一哉

1. はじめに

電子文書等のディジタルデータの存在時刻を保証するためのサービスとして，我が国では2000年前後から時刻認証サービスが事業化されている．時刻認証サービスが取り扱う時刻は時刻配信サービスによって日本標準時とのトレーサブルな関係が保証される．時刻認証業務と時刻配信業務を含む「タイムビジネス」が厳正に実施されていることは，一般財団法人日本データ通信協会の「タイムビジネス信頼・安心認定制度」により認定される．

2002年1月に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）」を端緒に[(1)]，2002年6月に設立されたタイムビジネス推進協議会及び2006年6月に設立されたタイムビジネス協議会（両者とも略称はTBF）が日本におけるこのようなスキームの構築や普及に貢献してきた．

近年，EU（欧州連合）におけるeIDAS規則（Electronic Identification and Trust Services Regulation：Regulation（EU）No 910/2014，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG）の制定や，データが重視されるSociety5.0による超スマート社会に対する取組み等の出現により，タイムビジネスのみでなく電子署名，eシール，送受信証明などを含むより広い概念である「トラストサービス」が注目を集めつつある．このような動向を捉え，筆者らはトラストサービス関連の標準化や制度化，普及促進に資するためTBFを発展的に改組し，2018年6月にトラストサービス推進フォーラム（TSF）を設立した（図1）．

本稿では，タイムビジネス及びトラストサービスの概要を紹介し，日本におけるトラストサービスに関連する課題と今後の展望について述べる．

2. タイムビジネス

2.1 タイムビジネスの定義と法的な位置付け

2004年11月5日に総務省より公開された「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～」（http://www.soumu.go.jp/main_content/000485112.pdf）で時刻配信業務，時刻認証業務，タイムビジネス及び時刻認証業務の定義の中でタイムスタンプがそれぞれ次のように定義されている．

（1） 時刻配信業務

情報通信ネットワークを利用する上で必要となるサーバ等の電気通信設備に用いられる時刻に高い信頼性を与えるため情報通信ネットワークを通じて時刻情報を配信する業務，更に配信先の時刻精度を計測して報告を行う時刻監査業務をいう．

（2） 時刻認証業務

電磁的記録（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって，電子計算機による情報処理の用に供されるものをいう．）に記録された情報（以下「電子データ」という．）に係る情報について行われる措置であるタイムスタンプ[(用語)]の付与及び当該タイムスタンプの有効性を証明する業務をいう．

宮崎一哉　トラストサービス推進フォーラム
E-mail　Miyazaki.Kazuya@dh.MitsubishiElectric.co.jp
Kazuya MIYAZAKI, Nonmember（JAPAN Trust Service Forum, Tokyo, 100-8310 Japan）.
電子情報通信学会誌　Vol.103 No.4 pp.402-406 2020年4月

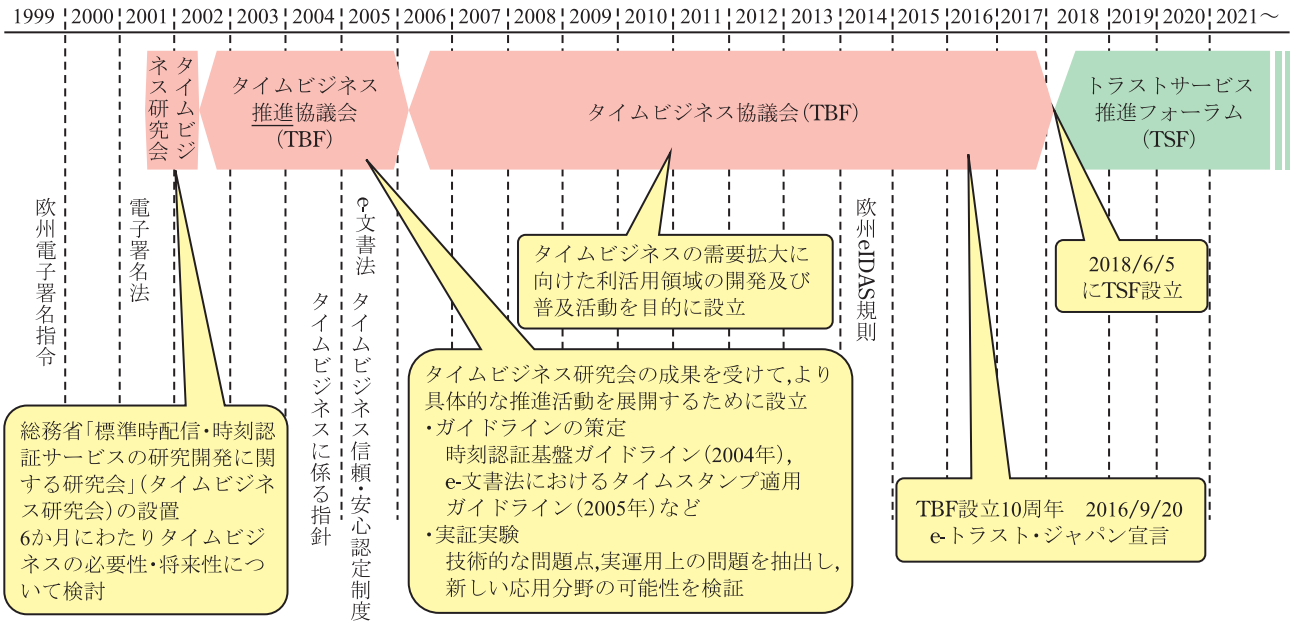

図1　TBF から TSF への推移　対象範囲をタイムビジネスに限定していた TBF を，より広い「トラスト」を対象とする TSF に発展的に改組した．

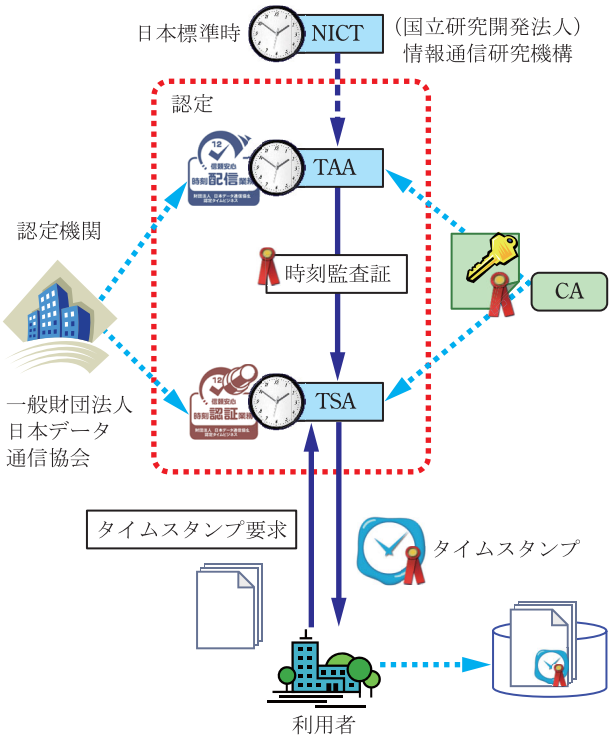

図2　タイムビジネスの構造　TAA 及び TSA は（一財）日本データ通信協会の「タイムビジネス信頼・安心認定制度」により厳正に業務が実施されていることが認定される．

用　語　解　説

タイムスタンプ　電子データがある時刻に存在していたこと及びその時刻以降に当該電子データが改ざんされていないことを証明できる機能を有する時刻証明情報．

（3）　タイムビジネス
「時刻配信業務」及び「時刻認証業務」の総称を指す．

「指針」には法的な意味合いはなく，本指針の場合，タイムビジネスに対する総務省の公式見解の位置付けである．日本にはタイムスタンプに関する法制度は存在しない．

2.2　タイムビジネスの構造

日本におけるタイムビジネスの構造を図 2 に示す．2.1（2）で説明した時刻認証業務は図 2 の TSA（Time Stamping Authority：時刻認証局）が，時刻配信業務は TAA（Time Assessment Authority：時刻配信局）が実施する．TSA は利用者からのタイムスタンプ要求を受け，タイムスタンプを生成し，利用者に返す．TSA がタイムスタンプ生成時に利用する時刻源は TAA により監査され，国立研究開発法人情報通信研究機構が生成する日本標準時との同期が図られる．TSA と TAA は，一般財団法人日本データ通信協会により，同協会が定めた技術，運用，設備等の基準を満たし厳正に業務が実施されているかの認定を受けることができる．日本における標準的な方式ではタイムスタンプ及び同期に利用される時刻監査証にそれぞれ TSA 及び TAA の電子署名が付与されるが，そのための公開鍵証明書は CA（Certificate Authority：認証局）が発行する（図 2）．TSA，TAA，CA をそれぞれ別組織とすることにより，結託を困難にする構造としている．

2.3　タイムビジネスに関連する技術及び標準

タイムビジネスに関連するデジュール標準にはISO/IEC 18014-1～4やITU-R Recommendation TF. 1876, JIS X 5094などがあるが，最も影響力のある規格がデファクト標準であるIETF（Internet Engineering Task Force：インターネット技術特別調査委員会）のRFC3161“Internet X. 509 Public Key Infrastructure Time-Stamp Protocol（TSP）”である．本規格はタイムスタンプのフォーマット及び利用者とTSA間のプロトコルを規定するものであり，幾つかのデジュール標準からも引用されている．

上記のうち，ISO/IEC 18014-4，ITU-R Recommendation TF. 1876，JIS X 5094はTAAとTSAの時刻同期に関わる日本発の標準であり，一般財団法人日本データ通信協会の認定要件としても利用されている．

3.　トラストサービス

3.1　トラストサービスの定義と法的な位置付け

EUではeIDAS規則で次の（1）～（3）がトラストサービスであるとして外延的な定義を与えている．

（1）　電子署名，eシール，タイムスタンプ，電子登録配布サービス，そしてそれらのサービスに関連した公開鍵証明書の生成，検証サービス

（2）　Webサイト認証のための公開鍵証明書の生成，検証サービス

（3）　電子署名，eシール，タイムスタンプ，あるいはそれらのサービスに関連する公開鍵証明書の保存サービス

電子署名は，日本における電子署名法（電子署名及び認証業務に関する法律）で言うところの電子署名に相当し，自然人が作成して，本人の意思を表明するために用いる．

eシールは法人や組織の電子署名であり，技術は自然人による電子署名と同等であるが，作成主体が自然人ではなく，法人や組織となる．eシールはそれが付与されたデータの発信元を証明するために用いる．eシールが「会社の意思」を表明できるか，契約に利用できるかなど，その効果については各国内法で規定される．

タイムスタンプは日本と同様，ディジタルデータの存在時刻及び非改ざんを証明するために用いる．

電子登録配布サービスは日本における内容証明郵便の電子版と考えればよく，送受信者の本人性，送受信内容，送受信時刻などの証明に用いる．

Webサイト認証はSSLサーバ証明書を用いてWebサイトを提供する組織の実在性や正当性を確認できるようにするものである．

このほか，関連する公開鍵証明書の発行や，電子署名等を検証・保存を行うサービスなどが定義されている．

一方，国内では，高度情報通信ネットワーク社会推進戦略本部が官民データ活用推進戦略会議により作成され，2019年6月7日に閣議決定された「デジタル時代の新たなIT政策大綱」（https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20190607/siryou1.pdf）において，トラストサービスを「データの存在証明・非改ざん性の確認を可能とするタイムスタンプや，企業や組織を対象とする認証の仕組みなど」と定義している．

両者ともトラストサービスをほぼ同一の概念と捉えている．これらを勘案して本稿ではトラストサービスを次のとおり定義する．

「トラストサービスとは，電子文書等のディジタルデータに関するある種の「トラスト」を証明するためのサービスである」

ディジタルデータに対して何らかの「トラスト」を与えたい，つまり何らかの証明を行いたい利用者は，トラストの内容により，適当なトラストサービス事業者（TSP）に対してリクエストを送付し，トークンを受け取る．得られたトークンをディジタルデータとともに依拠者や第三者等に渡すと，「検証」を実行し，結果として成功した場合にトラストの内容を受け入れる（図3）．

例えば，電子文書の存在時刻及び非改ざんという「トラスト」を証明したい場合，TSPである時刻認証事業者にトークンの一種であるタイムスタンプを要求する．依拠者等がタイムスタンプと電子文書を受け取り，タイムスタンプの検証に成功すると，電子文書がタイムスタンプに記された時刻に存在し，それ以降改ざんされてい

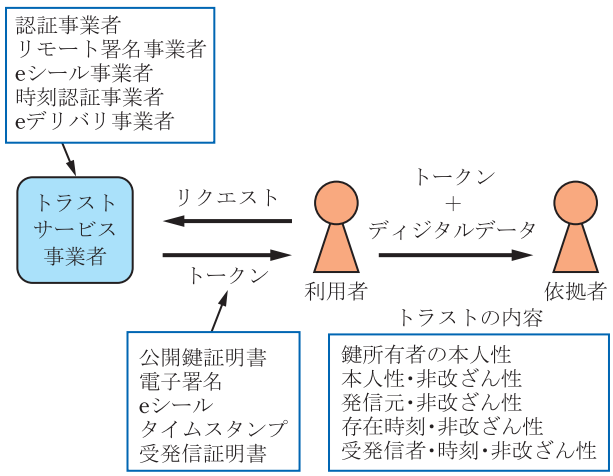

図3　トラストサービスの構造　ディジタルデータにトラストを与えたい利用者はトラストサービス事業者よりトークンを得，ディジタルデータに添付することで第三者にトラストを証明できる．

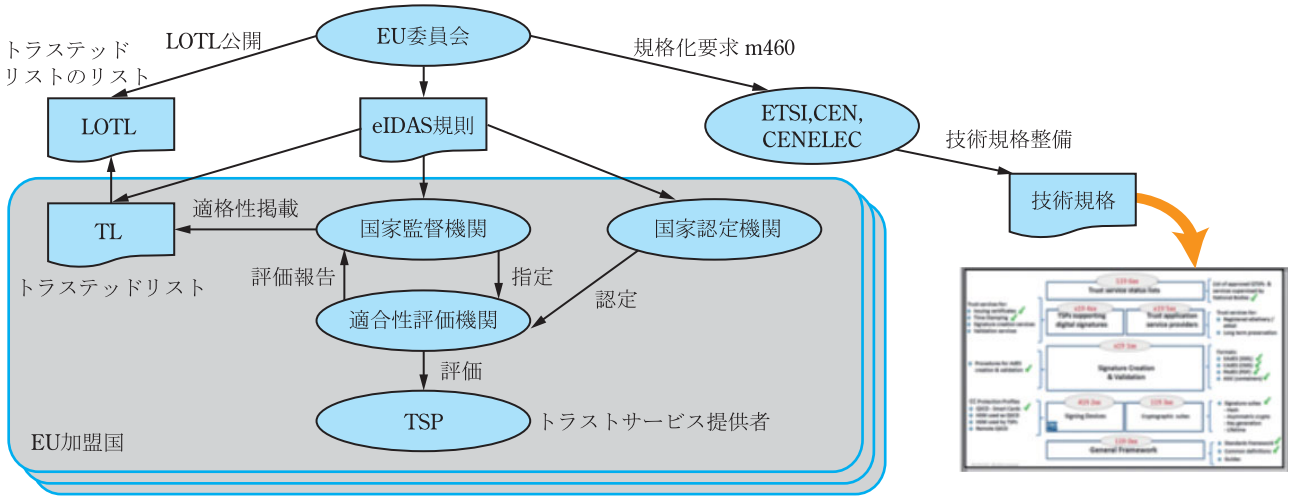

図4　EUにおけるトラストサービスのためのフレームワーク　EUでは法制度，監督・監査，標準化体制，トラステッドリストにより，トラストを成立させている．

ないことを受け入れる．

この際，「検証」の内容が「トラスト」を特徴付けるポイントとなる．

依拠者等による検証の内容は次の2点のみである．

① トークンが信頼できるTSPより発行されていること
② トークンが改ざんされておらず有効であること

時刻認証事業者について①は「タイムビジネス信頼・安心認定制度」の認定を受けていることを確認すればよく，②についてはPKI（公開鍵基盤）の標準的な技術を用いた検証ソフトを利用すればよい．

つまり，TSPの信頼性や利用する技術の信頼性（暗号アルゴリズムの安全性など）については依拠者等が自ら検証することはせず，他の何らかの保証手段に委ねることになり，これが「トラスト」と呼ぶゆえんである．

TSPの信頼性を保証する手段としては，評価や監査を経た認定，法令，契約等が考えられる．また，技術の信頼性については国際標準規格等が考えられる．

3.2　EUにおけるトラストサービスのためのフレームワーク

EUではトラストを成立させるため，図4に示すフレームワークを構築し，運用している．

このフレームワークでは，eIDAS規則という法制度の下，国家認定機関が認定した適合性評価機関がTSPを評価し，決められた基準を満足していれば，国家監督機関が信頼できるトラストサービスとしてトラステッドリストに掲載する．トラステッドリストはXMLで記述された機械可読な情報であるため検証ソフトがそのまま検証処理で利用できる．評価・監査は定期的に実施され，トラステッドリストは常に最新の状況が維持される．これによりTSPの信頼性は各国及びEUが公的に確認可能としている．技術の信頼性を確保するために，EUがETSI（欧州電気通信標準化機構），CEN（欧州標準化委員会），CENELEC（欧州電気標準化委員会）などに対し，法制度と整合性の取れた技術標準の作成と維持を命じている．

表1　日本のトラストサービスの状況

	電子署名	タイムスタンプ	その他（eシール，eデリバリなど）
法令	あり	なし	なし
認定	あり	あり	なし
評価機関	主務大臣指定	民間	なし
標準化体制	なし	なし	なし
信頼できる業務の表示	機械可読なし（ルート証明書のフィンガープリント）	機械可読なし（事業者名のみ）	なし

4.　日本における課題と今後の展望

欧州では3.1の（1）～（3）に挙げたトラストサービスに対してeIDAS規則によって法的根拠を与え，図4に示したフレームワークを共通のフレームワークとして個々のトラストサービスに提供し，「トラスト」を維持できるようにしている．

一方日本では，電子署名，タイムスタンプ，その他のトラストサービスで状況が異なっているばかりか（表1），トラストを成立させるためにはいずれも満足できるものではない．特にビジネスがグローバル化しつつある現状においては，日本のトラストサービスを海外で通用

させることを視野に入れた検討が必要である．

この状況を打開するため，総務省は2019年1月，プラットホームサービスに関する研究会の下にトラストサービス検討ワーキンググループを立ち上げ，トラストサービスの制度化に関する検討を実施している．執筆時点で第13回まで会合が開催され，リモート署名，eシール，タイムスタンプ，Webサイト認証，eデリバリなどの個別の議論に加えトラストサービス全体の制度化に関わる議論などを積極的に重ねている（http://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html）．前述した「デジタル時代の新たなIT政策大綱」では，「トラストサービス（データの存在証明・非改ざん性の確認を可能とするタイムスタンプや，企業や組織を対象とする認証の仕組みなど）の活用のための制度の在り方を含め，関係省庁間で連携し，法令に基づき民間企業等が行う文書保存等の一層のデジタル化に向けた取組について検討を行い，令和元年度内に結論を得る．」としており，トラストサービス検討ワーキンググループでは2019年内には検討結果を最終報告書案としてまとめる見通しである．

Society5.0が目指す，「データ駆動」により新たな価値を創出する超スマート社会を実現するためには，セキュリティに加えて「トラスト」が重要な役割を担うことは論をまたない．トラストサービス推進フォーラムとしてはEUの動向等を注視しつつ，日本らしい「トラスト」の基盤構築に向けて尽力していく．

文　　献

（1） 岩間　司，齊藤春夫，町澤朗彦，鳥山裕史，“日本のタイムビジネスの動向，”情報通信研究機構季報，vol. 56, nos. 3/4, pp. 65-78, Sept. 2010.

（2019年11月7日受付）

宮崎　一哉（みやざき　かずや）

昭57東工大・工・制御卒．昭59同大学院総合理工学研究科修士課程了．同年三菱電機株式会社入社．以来，分散アプリケーション，公開鍵暗号基盤の研究に従事．現在，同社生産技術部．トラストサービス推進フォーラム副会長．著書「電子文書保存のしくみと実務」など．

5月号特集予定目次

「様々なハードウェアに適応したAI実装技術」