信頼されるタイムスタンプサービス

遠隔管理方式に関する技術・運用基準検討報告書

（概要版）

平成20年12月

タイムビジネス協議会

はじめに

タイムビジネス信頼・安心認定制度が設立され、タイムビジネス推進協議会が「信頼されるタイムスタンプ技術・運用基準ガイドライン」を公開して以来、すでに約3年が経過し、当初の基準において想定されていたサービス内容を越えて市場からの要求は広がっている。例えば電子商取引分野では長期署名に付与され、医療分野では医療情報の電子的な証拠性確保に用いられ始めるなど、ユーザが要求するサービスレベル、コストは極めて多様化している。この現状に対してタイムスタンプサービス事業者が単一の運用ポリシー、設備で対応していくにはコスト、運用の制限を受ける可能性があり、結果として市場、ユーザからの要請に適応できない場合が想定される。

本WGでは、タイムスタンプ事業者が管理するタイムスタンプユニット（TSU）をユーザ設備内に設置する方式である「遠隔管理方式」タイムスタンプサービス（Managed Time Stamping Service 以下MTSサービス）の技術・運用上の課題を明らかにすることを目的とする。信頼・安心のレベルを維持したまま、ユーザ設備内で直接タイムスタンプを発行するサービスの提供が可能で多様な市場要求に対応できるかを検討した。

本報告書の内容に関しては更なる議論を要する点を含むが、今後の認定基準、サービス事業者の運用改善の一助となることを願うものである。

目　　次

１．MTS サービスの全体像

１．１　MTS サービスのモデル

現在、一般的に利用されているタイムスタンプサービスは、安全に管理運用されたタイムスタンプ局に対して、インターネットまたはその他の通信手段を介して、ユーザがタイムスタンプ要求を行う形式である。

このようなサービスは、広範なユーザ層に対してあまねくサービスを提供することに適している一方、下記のような要求に対して十分な解を提示できないことが想定されている。

[利用目的]

○ネットワークセキュリティの向上

タイムスタンプを生成する際、電子文書のハッシュ値のみタイムスタンプ局に送付されるが、そのような送付した事自体も外部に秘匿しておきたい場合。インターネットへのセキュリティ上の不信感による要求。

○通信手段の途絶時への対応

災害時など通信手段の途絶時にタイムスタンプ利用が行えなくなる結果、ユーザシステムの停止を招く恐れがあることへの対策。

○大量かつ高速なタイムスタンプ付す

銀行等における大量の月次伝票、企業におけるメール通信や EDI などのトランザクションデータにタイムスタンプを付す場合等。

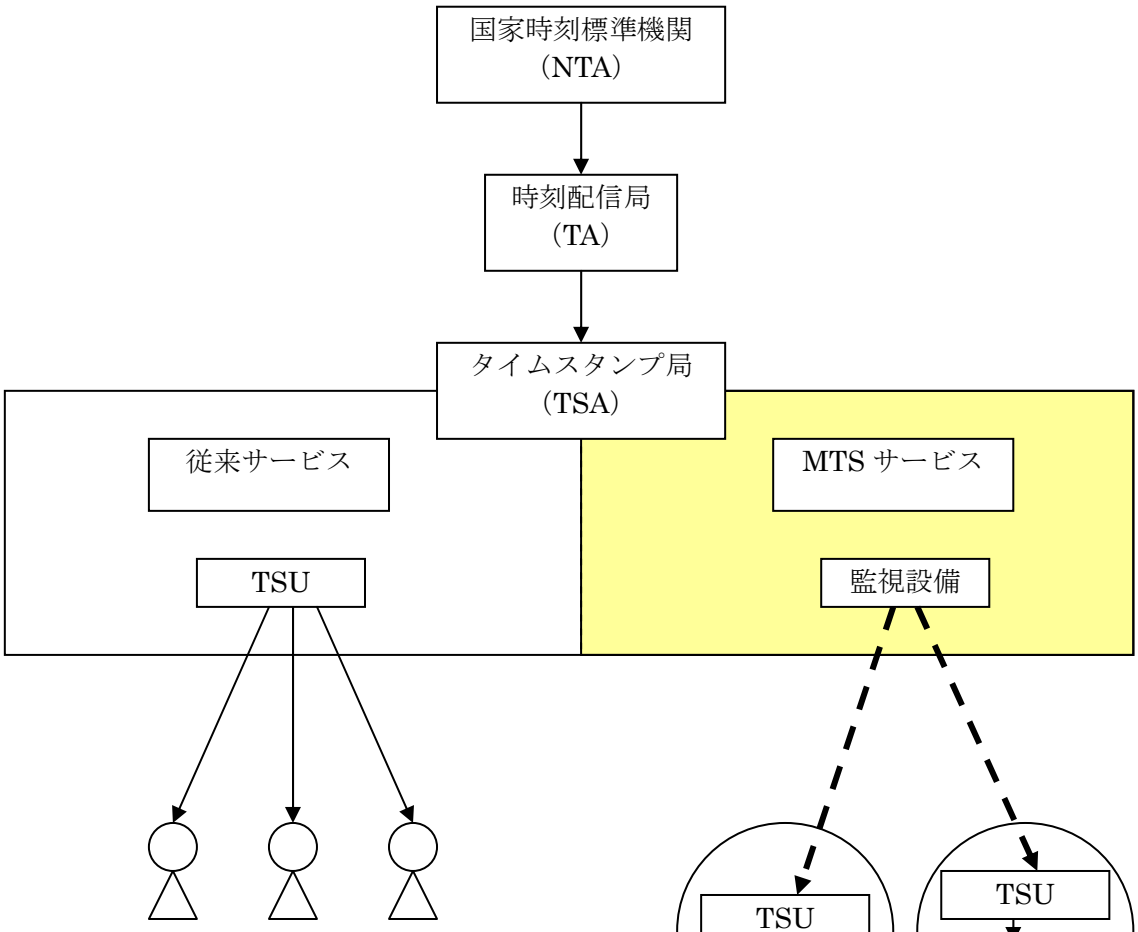
○サービスレベルが異なるサービス提供が求められる場合

サービス提供時間や可用性、応答速度などのサービスレベルが異なる要件が混在している場合、サービス事業者はもっとも高い要求に合致させる必要があるため、結果的にサービスコストが高くなる可能性がある。

上記のような要求に対して、ユーザ毎に独立の TSU をユーザシステム設備内に設置することで解決するのが本報告書で検討する MTS サービスのモデルである。

流通したタイムスタンプは、サービスの運用形態にかかわらず、同じ効力を持たねばならない。このため、既存のタイムスタンプサービスの信頼性・安全性が維持されることが必要である。

このため本検討では、既定の認定基準を承認されたタイムスタンプ事業者が、既存のサービスに追加する形で MTS サービスを行う事業形態を前提とする。



タイムスタンプユニット（TSU）は、タイムスタンプ局内に設置・管理される。

タイムスタンプユニット（TSU）は、ユーザ設備内に設置され、タイムスタンプ局から遠隔監視、操作が行われる。

１．２　ETSI による MTS サービスの定義

ETSI TS 102 023 v1.2.1(2003-01)では、MTS サービスを次のように説明している。

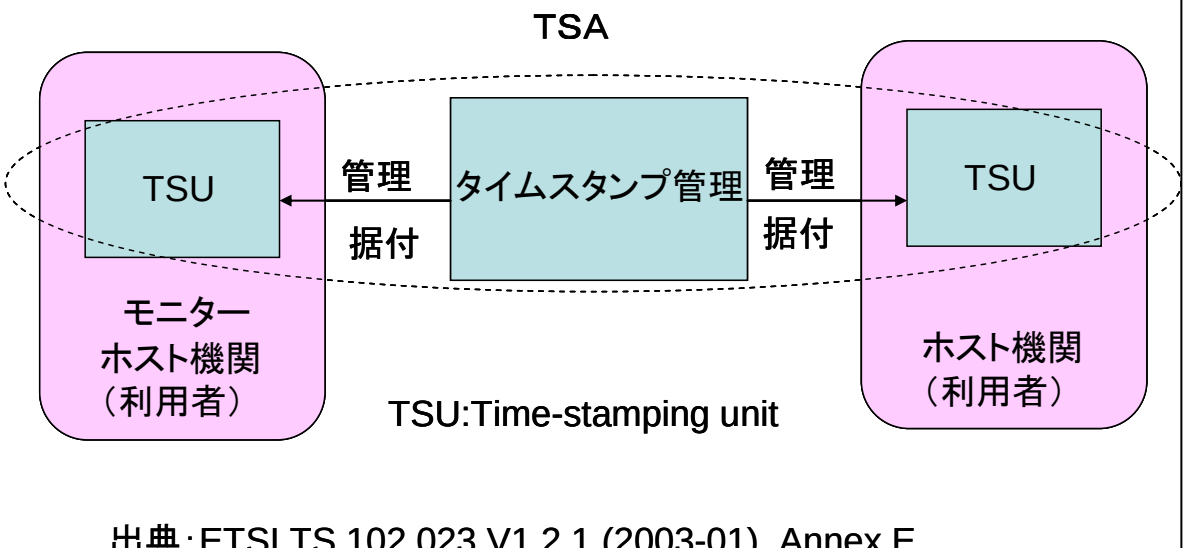
組織によっては、TSU の設置、操作、管理は外部機関に委託する一方、高品質なタイムスタンプサービスを近接した状態で受けるために、複数の TSU を組織内で受け入れたいという要望がある。

このサービスは、受け入れ組織の構内に設置された TSU を、TSA が遠隔管理し、サービス品質の全責任を TSA が取る形態で実現できる。

ETSI のこの文書(TSA に要求されるポリシーについて記述している)で記載のタイムスタンプサービスの要求は、タイムスタンプ生成の管理と、TST (Time-Stamp Token)を発行する TSU の操作の両者への要求となっている。TST の中で識別される TSA はこれらの要求を満足している事を保証する責任がある(例えば、契約義務等により)。

受け入れ組織は、通常サービスの利用の監視と、少なくともサービスが稼動しているかを、更にはサービスの実績、例えば、ある期間に生成されたタイムスタンプの数の計測が可能となる事を希望することは明白である。このような監視は、タイムスタンプサービスの範疇外と考えられる。

それゆえに当該 ETSI 資料の主要部に記載の管理操作の記述は、規制とはならない。TSU に対して直接なされる監視操作は、TSA により許可されうる。MTS の概念図を、図 1 に示す。



出典：ETSI TS 102 023 V1.2.1 (2003-01), Annex E

図 1　ETSI MTS の概念図

２．本 WG の検討結果

２．１　定義・要件

本検討では、財団法人日本データ通信協会の認定を受けることのできるデジタル署名技術を使用する方式の MTS サービスを対象とした。これは、現時点において MTS サービスが利用されるにあたり、最も導入が容易と考えられる方式であるためである。

MTS サービスにおいても認定された TST を発行するためには、最低条件として発行された TST の信頼性が、従来の認定タイムスタンプ局発行の TST と同等であることが必要である。そのために求められる要件を以下に具体的に示す。

(1) マネージメントする主体

タイムスタンプサービスとしての信頼性を保証するために、遠隔地に設置される機器を含めた全ての認定対象機器のマネージメントの責任主体は、タイムスタンプ事業者である必要がある。従来の認定レベルと同等であることを示すために、MTS サービスを行うタイムスタンプ事業者は、既存の認定を取得している必要がある。

(2) M-TSU（MTS サービスで使用される TSU）の管理者

M-TSU の管理は、MTS サービスの信頼性維持に不可欠のものであり、責任を負うべきマネージメント主体（認定タイムスタンプ局）が管理することが必要である。

(3) M-TSU の所有者

管理者（マネージメント主体：認定タイムスタンプ局）の管理に影響を与えない限りにおいては、M-TSU の所有権を制限する必要性は認められないため、所有権に関しては、限定されない。

(4) TSA 証明書

責任を負うべきマネージメント主体が TSA 証明書の Subject DN に明示される必要があり、かつ、MTS サービスとして発行されたことを明示しなければならない。さらに、MTS サービスの適用範囲を明確にするために既存のタイムスタンプサービスの TSA 証明書と区別する必要がある。なお、MTS サービスの TSA 証明書に MTS ユーザのシステム名等が記述されることを妨げない。

(5) 秘密鍵の管理（保管・運用等）主体

秘密鍵の管理は、TST 発行の管理で最も重要な事項であり、責任を負うべきマネージメント主体（認定タイムスタンプ局）が管理することが必要である。

(6) 認定を受ける主体（認定申請者）

MTS サービスにおいて、その責任を負うものは管理を行う認定タイムスタンプ局である。既存の認定基準によるタイムスタンプ局の認定を受けることで、M-TSU を制御する設備の信頼性と M-TSU の発行する TST の信頼性は担保できる。このため MTS サービスにおける認定申請者は、既存の認定タイムスタンプ局であることが必要である。

(7) M-TSU の設置場所

管理者（マネージメント主体：認定タイムスタンプ局）の管理に影響を与えない限りにおいては、M-TSU の設置場所を制限する必要性は認められないため、設置場所に関しては、限定されない。

(8) MTS ユーザの範囲

MTS サービスはユーザシステムに M-TSU が設置され特定のアプリケーションサービスまたは、法人内で利用されることを前提としている（P6:補足参照）。MTS ユーザは個別の契約などにより運用条件を特定可能な範囲に限定されるため、不特定多数へのサービス提供は認められない。

(9) M-TSU 発行 TST 検証者

TST の信頼性が、従来の認定タイムスタンプ局が直接発行する TST となんら変わらないものであり、検証者を限定する必要性はない。

以上をまとめた表を以下に示す。

網掛けした部分が本ガイドラインで検討している MTS サービスの要件を示す。

(1)マネージメントする主体

a	b	c
認定 TSA	認定 TSA 以外	限定しない

(2) M-TSU の管理者

a	b	c
認定 TSA((1)の主体)	MTS ユーザ	限定しない

(3) M-TSU の所有者

a	b	c
認定 TSA((1)の主体)	MTS ユーザ	限定しない

(4) TSA 証明書

a	b	c
認定 TSA((1)の主体)	MTS ユーザ	限定しない

(5) 秘密鍵の管理（保管・運用等）主体

a	b	c
認定 TSA((1)の主体)	MTS ユーザ	限定しない

(6) 認定を受ける主体（認定申請者）

	b	c	d
認定 TSA((1)の主体)	MTS ユーザ	両者	限定しない

(7) M-TSU の設置場所

a	b	c
認定 TSA((1)の主体)	MTS ユーザ	限定しない

(8) MTS ユーザ（TST 発行要求者）の範囲

a	b	c
1 ユーザに限定	契約等により 1 ユーザと見なされる範囲	限定しない

(9) M-TSU 発行 TST 検証者

a	b
1 ユーザに限定	限定しない

以下に本章で述べた要件の図解を示す。

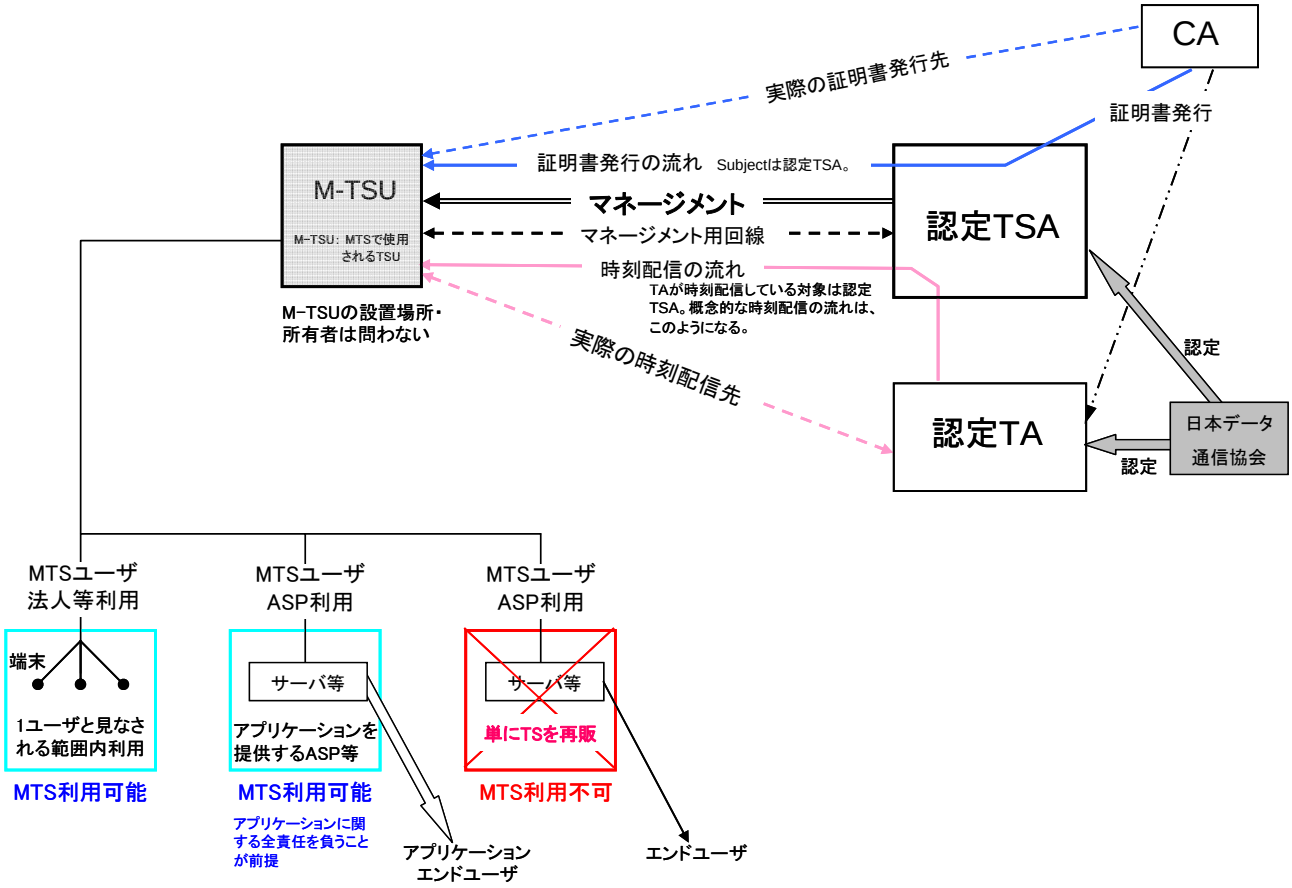


図 2　MTS サービス概念図

補足

MTS サービスを利用できるユーザの範囲は、技術的課題よりも運用面で認定制度の根幹に係る問題を含んでいる。

従来の認定タイムスタンプ局の審査基準では、当該サービスの安定したサービス提供のためにハードウェアの冗長構成、ソフトウェアの安定性、ファシリティの耐震･耐火性や防火設備の設置、運用管理体制（運用ポリシー等の規定整備、訓練・障害復旧体制の確立）等に関して、厳しい規定が定められている。これらは、当該サービスは、広く一般の不特定多数に利用されるものであり、そのサービスの停止はユーザにとって大きな支障となるために高い可用性を求めているためである。

これに対して、MTS サービスは、認定タイムスタンプ局が直接発行する TST と同等の信頼性を有している TST が必要なニーズの中で、TSU をユーザ側に設置することにより、高速性や高いセキュリティを求めるユーザによって使用されるものである。このため、認定タイムスタンプ局の MTS サービスにおいても他の MTS サービスと同様にその利用範囲（TST を要求・利用するユーザの範囲）は、限定的なものが多数を占めると考えられる。

逆に認定制度の信頼性維持の観点からは、認定タイムスタンプ局の MTS サービスを不特定多数にその利用を認めた場合、上記のように高い可用性のために認定基準が厳しいものを課す必要がある。多くの想定される MTS ユーザは自らの管理する範囲に M-TSU が

設置されており、そのファシリティの管理も出来る状態である。このため、可用性の一部は、MTS ユーザ側が部分的に責任を持つことが可能なことを示している。

これらより、認定タイムスタンプ局の MTS サービスのユーザを限定することによって、認定制度の信頼性を維持したまま、認定基準の緩和が可能になり、より簡便な設備で MTS サービスが利用可能となる。ここで基準緩和した部分に対する担保は、ユーザが限定的であることにより、認定タイムスタンプ局と MTS ユーザ間の契約行為により解決できるものと考える。この基準緩和は、認定タイムスタンプ局の MTS サービスの利用・普及に貢献するものである。

３．認定基準への適用

３．１　概要

「タイムビジネス信頼・安心認定制度」に係るタイムスタンプは、e-文書法の施行に伴い、「電子帳簿保存法施行規則」及び「地方税施行規則」において、国税関係及び地方税関係書類の電子保存の義務的要件として明文化されている。また。同様に両施行規則において、電子取引における取引情報の電子保存の選択肢の１つに、同タイムスタンプを付すことが義務的要件として規定されている。

本報告書で検討する MTS サービスも、両施行規則で想定しているタイムスタンプと同等の品質が要求される。このようなことから、現在のデジタル署名を使用する方式の認定基準を出発点として、MTS サービスの特徴を考慮した場合、どの基準項目を緩和できどの項目を新規に追加すれば、現在のサービスと同等の品質を保てるかという観点から検討を加えた。

３．2　認定基準に対する検討項目

本報告書では、現在ある「タイムビジネス信頼・安心認定制度　認定基準」を検討対象とし、MTS サービスを導入するために必要な変更点を識別した。これは、現在のガイドラインが既に発行から 2 年半を経過しており、現状に合わなくなった部分があること、及び認定基準にはある規定に該当する部分が、ガイドラインにはない項目があるため、認定基準を検討対象にすることで、より詳細な検討が行えるためである。

以下の根拠により、現行の認定基準から緩和・追加すべき項目を識別した。

【緩和項目】

① 契約により担保出来るために緩和できる項目

従来の認定タイムスタンプ局が行っていたタイムスタンプサービスは、不特定多数のユーザを対象としていたのに対して、MTS サービスでは、個別に MTS ユーザとサービス提供の条件（サービス提供時間、サービス一時停止・終了の事前通知義務など）を取り決め、サービスを提供する。この際には契約行為が伴い、この契約に関係する規定が含まれていることのみの審査で緩和することが可能となり、本項目はこれに該当する審査項目である。

②MTS ユーザが容認できる可用性レベルにより緩和できる項目

多くの想定される MTS ユーザは自らの管理する範囲に M-TSU が設置されており、そのファシリティの管理も出来る状態である。このため、可用性の一部は、MTS ユーザ側が部分的に責任を持つことが可能なことを示しており、また、その責任をどこまで認定タイムスタンプ局が負うかは契約によって定めることにより、緩和することが可能である。本項目はこれに該当する審査項目である。

③個人情報に関する緩和できる項目

MTS サービスでは、認定タイムスタンプ局が MTS ユーザと 1 対 1 で主に法人契約を結ぶものであり、従来のサービスと異なり、個人情報が認定タイムスタンプ局にもたらされるものではない。本項目はこのために緩和することが可能な審査項目である。

【追加項目】

①契約による担保で緩和した項目に関しては、当該項目が契約に含まれているかを審査する項目を追加した。

②MTS ユーザによる不正の防止を行うためにマネージメントが中断した場合（回線断等）に M-TSU が停止する機能を有することを審査する項目を追加した。

③MTS ユーザ（TST 発行要求者）は、契約等によって、その MTS サービスの範囲が限定されていることから、単純な TST の再販は認めないことが適当と考えられる。

３．３　議論

本 WG の検討で行われた主な議論

MTS サービスであることの明示

MTS サービスは、汎用タイムスタンプサービスと異なる基準、運用に基づいている。このため、タイムスタンプの検証者が容易にサービスの違いを識別できる必要があると考えられる。このため

・MTS で用いられる TSA 証明書には、MTS であることを明示すべきであるとの議論がある。
・MTS 毎にユニークなポリシーOID が記述されるべきであるとの議論がある。

マネージメントされていることの証明

MTS では M-TSU がユーザシステム内に設置されることが想定されている。同一の認定基準を保つには M-TSU およびその関連設備の管理・監視が、汎用タイムスタンプサービスと同じレベルで実施されている必要があるが、これを証明する技術面、運用面からの基準が必要である、との議論を行った。

その議論から、MTS サービス特有の基準案が追加されているが、認定審査時に個別に検証される事項と考え、本報告では具体的な基準内容には言及していない。

マネージメントされる対象範囲

参考情報として挙げている ETSI の概念図では、あたかも M-TSU のみがユーザ先に設置され、TSA からの管理を受けるかのように見える。しかし、認定基準や既存 TSA のシステム内容からは、TSU 以外の様々なネットワーク設備、サーバ類が M-TSU に付属してユーザ設備内に設置されることが想定される。

これらの付属設備に関しても認定審査の対象である場合､TSA 局側からのマネージメントの対象の具体的な範囲を明確化する必要があるとの議論がある。

有用性に関しての議論

MTS に対する需要として、災害時など時刻配信局との通信が途絶した場合でも独立して運用ができることが望ましい、というものがある。

本検討での MTS では､マネージメントをおこなう TSA との接続が維持されている必要があるため、上記要件は現状満たせない。ただし、無線（モバイル）などの狭帯域の回線でも M-TSU のマネージメントは継続が可能であると考えられるため、MTS ユーザが大量のタイムスタンプ発行要求を行ったとしても、ユーザシステムと近接している M-TSU 自体は、マネージメント回線の帯域に依存せずにタイムスタンプ発行を継続できるメリットがある。これらの議論は第 1 章 1 項「MTS サービスのモデル」に反映した。

アプリケーション制限の議論

本検討では MTS 利用者と TSA 間の個別契約によって責任範囲を特定することで基準の緩和を行っている。この代償として MTS 利用者による、タイムスタンプの単純な再販を認めていない。これは、障害発生時にエンドユーザに対する責任の所在が不明瞭になる可能性を考慮している。しかし、MTS 利用者がタイムスタンプをどのように扱うかで基準適用範囲が異なるとする場合の判別基準はより明確にされなければならないとの議論がある。

認定を受ける主体（認定申請者）に関する議論

MTS サービスにおいて、その責任を負うものは管理を行う認定 TSA であり、TSA 単独で申請し、認定を受けることで M-TSU の発行する TST の信頼性は担保できるため、認

定申請者は、TSA とすることが必要であるとした。
これは、M-TSU は、MTS ユーザの管理範囲（MTS ユーザの社内等）に置かれる（第3者管理範囲の場合もあり。）が、設置場所のファシリティの管理者である MTS ユーザ等も認定申請の対象とすることは、過剰な負担となり、認定 TSA の MTS サービスの利用・普及の妨げとなる可能性が高いという議論に基づく。

ファシリティ基準
MTS サービスでは、サービスの継続性に関しては MTS 利用者との個別契約によって調整可能であるとの考えから、契約内容を審査基準に追加することで、ファシリティ基準の緩和を行った。M-TSU は認定事業者が直接関与できない場所に設置されるが、M-TSU は耐タンパ性を持った「安全な装置」という前提で、緩和が可能ではないかという議論がある一方で、遠隔管理に伴うリスクを考慮し汎用タイムスタンプサービスより厳しい基準が必要であるとの議論もあった。

３．４　「タイムビジネス信頼・安心認定制度」認定基準への検討結果適用例

（非公開）

参考

ETSI TS 102 023 V1.2.1 (2003-01), Annex E
http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_102023v010201p.pdf

タイムビジネス信頼・安心認定制度
時刻認証業務の審査基準：時刻認証業務（デジタル署名を使用する方式）
http://www.dekyo.or.jp/tb/summary/data/D-criteria3rdVHP0805.pdf

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　ホームページ
http://www.dekyo.or.jp/tb/index.html

本検討会参加メンバー（五十音順）

主査	セイコープレシジョン株式会社	中嶋　勝治
主査	日本電気株式会社	酒井　雅啓
	アマノタイムビジネス株式会社	市川　桂介
		小田　　聡
	株式会社インターネットイニシアティブ	三膳　孝通
	インターネットマルチフィード株式会社	稲葉　秀司
		田口　裕真
	独立行政法人情報通信研究機構	岩間　　司
		鳥山　裕史
	セイコーインスツル株式会社	上畑　正和
		柴田　孝一
		村尾　進一
	セイコープレシジョン株式会社	浜原　研作
	セコムトラストシステムズ株式会社	西山　　晃
	日本電気株式会社	後藤　　淳
	株式会社ＰＦＵ	石川　昭一
		今井　秀和
		友田　大崇
	丸文株式会社	米川　知希
	三菱電機株式会社	宮崎　一哉

財団法人 日本データ通信協会
タイムビジネス協議会

〒170-8585　東京都豊島区巣鴨2-11-1　巣鴨室町ビル7階
Tel　:　　050-5508-1618
E-Mail：h-ishii@dekyo.or.jp
URL：　http://www.dekyo.or.jp/tbf/