コンピュータセキュリティ　17－6
（２００２．５．２３）

タイムスタンプ方式の検証手続の可用性による分類

宇根　正志[†*]　　**松本　勉**[†‡]
une@mlab.jks.ynu.ac.jp　　tsutomu@mlab.jks.ynu.ac.jp

†横浜国立大学大学院 工学研究科　**‡横浜国立大学大学院 環境情報研究院**　***日本銀行 金融研究所**

あらまし　本稿では，検証手続の可用性に焦点を当ててタイムスタンプ方式の分類方法について論じる．まず，検証手続の可用性の観点からタイムスタンプ方式を分類する際にどのような尺度が適当かを検討し，タイムスタンプの検証者が他のエンティティから検証に用いるデータを入手できない場合に実行可能な検証処理数を採用する．次に，実行可能な検証処理数によってタイムスタンプ方式を 10 の集合に分類する．最後に，7 つの既存のタイムスタンプ方式に対して本稿での検討結果を適用し，検証手続の可用性に関する特徴を明らかにする．

Classification of Time Stamping Schemes from the Viewpoint of Availability of Verification Procedures

Masashi Une[†*]　　Tsutomu Matsumoto[†‡]
une@mlab.jks.ynu.ac.jp　　tsutomu@mlab.jks.ynu.ac.jp

†Graduate School of Engineering, Yokohama National University　‡Graduate School of Environment and Information Sciences, Yokohama National University　*Institute for Monetary and Economic Studies, Bank of Japan

Abstract　This paper discusses the classification of time stamping schemes by the availability of verification procedures. First, we discuss what criterion is suitable to classify schemes by the availability. After considerable discussion, we choose, as the criterion, the number of feasible verification operations under situations in which a verifier cannot obtain data for the verification from other entities. Next, we classify schemes into ten categories by the number of the feasible operations. Finally, we apply our results to seven existing schemes and clarify their characteristics on the availability of verification procedures.

1　はじめに

タイムスタンプ技術は，特定のデータが特定の日時に存在したことを証明する技術である．近年の電子商取引の利用拡大等に伴ってタイムスタンプ技術の重要性に関する認識が高まってきており，Digital Notary[7] /SecureSeal[5]をはじめとする各種タイムスタンプ・サービスが開始されている．

こうした中，タイムスタンプ方式の評価に関する研究が進められている．Une and Matsumoto[10]は，タイムスタンプ方式の評価の枠組みを提案した上で，タイムスタンプの改ざん攻撃に対する安全性と，タイムスタンプ方式の実装に伴うコストの観点から各方式の評価を行った．また，宇根・松本[9]は，タイムスタンプ方式の可用性を定義した上で，タイムスタンプの発行・検証手続が正常に完了しないケースを整理し，検証者が検証に用いるデータを他のエンティティから入手できない場合に実行可能な検証処理を示した．

本稿では，宇根・松本[9]をベースに可用性の観点からタイムスタンプ方式の分類方法について検討する．具体的には，検証手続の可用性に着目した分類の尺度として，検証者が他のエンティティから検証に用いるデータを入手不可能な場合に実行可能な検証処理数を採用する．その上で，タイムスタンプ方式を 10 の集合に分類するとともに，7 つの既存のタイムスタンプ方式に本検討結果を適用し，それらの方式における検証手続の可用性上の特徴を明らかにする．本稿における検討結果は，タイムスタンプ方式の可用性を評価する際にどのような尺度を用いる

ことが有用かを示すものであり，タイムスタンプ方式の利用者がタイムスタンプ方式を評価する際に参考にすることができると考えられる．

まず 2 では，Une and Matsumoto[10]が提案したタイムスタンプ方式の枠組みを紹介する．3 では，宇根・松本[9]の検討結果を紹介した上で，本稿における検討の範囲を説明し，検証手続の可用性に着目してタイムスタンプ方式を分類する場合，どのような尺度を用いることが適当かを検討する．4 では，実行可能な検証処理数によってタイムスタンプ方式を 10 の集合に分類し，7 つの既存のタイムスタンプ方式に検討結果を適用する．5 では，本稿の結果を整理した上で，今後の課題を示す．

2 Une and Matsumoto [10]におけるタイムスタンプ方式の評価の枠組み

2.1 エンティティ

- **発行者**（time stamp issuer）：タイムスタンプを発行し，タイムスタンプやその発行・検証に用いられるすべてのデータを保管するエンティティ．複数のエンティティが協力して 1 つのタイムスタンプを発行する場合, それらを 1 つの発行者とみなす．また，タイムスタンプの検証に利用される 2 種類のデータ E_{TSI} と E_{AMP} を生成する場合がある．E_{TSI} は，タイムスタンプを構成するデータと発行者のデータベースのデータとの整合性を確認するデータである．E_{AMP} は E_{TSI} の一貫性を確認するデータであり，後述の証拠補強者に送付される．なお，発行者は，必要とされる精度の日時データ T を常に入手するものとする．
- **検証者**（verifier）：タイムスタンプや他のエンティティから得たデータを用いて, あるデータ M がある時点 T に存在したことを確認するエンティティ．
- **証拠補強者**（evidence amplifier）：E_{AMP} を発行者から入手・保管し，検証時に検証者に提供するエンティティ．E_{AMP} を安全に保管して E_{TSI} の証拠性を補強する役割を担う．
- **発行依頼者**（time stamp requester）：あるデータ M に対するタイムスタンプの発行を発行者に依頼するエンティティ．タイムスタンプに E_{ORE} が含まれる場合，別のタイムスタンプの検証時に E_{ORE} を検証者に送る．E_{ORE} は，E_{TSI} の一貫性を確認するデータである．
- **証明者**（prover）：あるデータ M が T の時点に存在したことを証明するために，M に対するタイムスタンプを検証者に送るエンティティ．

2.2 タイムスタンプを構成するデータ

タイムスタンプを，「特定のデータ M が特定の日時に存在したことを証明する目的で生成され，少なくとも H と ID_{TSI} を含むデータ」と定義する．H は M のハッシュ値，ID_{TSI} は発行者の識別データである．また，以下の T，$Info_{INT}$，E_{TSI}，E_{ORE}，ID_{REQ}，ID_{AMP}，

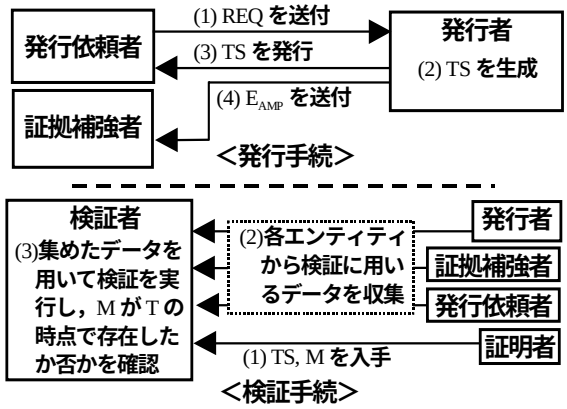

図 1 タイムスタンプの発行・検証手続

ID_{ORE} の各データもタイムスタンプを構成する場合がある．

- T：発行者が発行依頼者からタイムスタンプ発行要求データ REQ(H や発行依頼者の識別データ ID_{REQ} 等から構成）を受信する日時データ．
- $Info_{INT}$：タイムスタンプを構成するデータのうち，$Info_{INT}$ を除くデータを用いて生成され，それらの一貫性を確認するデータ．
- ID_{REQ}：発行依頼者の識別データ．
- ID_{AMP}：証拠補強者の識別データ．
- ID_{ORE}：E_{ORE} を含むタイムスタンプを有する発行依頼者の識別データ．

2.3 発行手続（図 1 上参照）

(1)発行依頼者は REQ を発行者に送付.
(2)発行者はタイムスタンプ TS を生成.
(3)発行者は発行依頼者に TS を送付.
(4)発行者は E_{AMP} を証拠補強者に送る場合もある．

2.4 検証手続（図 1 下参照）

(1)証明者は，少なくともデータ M と M に対応するタイムスタンプ TS を検証者に送付.
(2)検証者は，各エンティティから検証に用いるデータを収集.
(3)検証者は，一定の検証手続を実行し，その結果から M が T の時点に存在したか否かを確認.

2.5 検証手続を構成する 6 つの処理 a～f

- **処理 a**：検証者がタイムスタンプを構成するハッシュ値 H とデータ M のハッシュ値を比較する．
- **処理 b**：検証者が $Info_{INT}$ を用いてタイムスタンプを構成するデータ（$Info_{INT}$ を除く）の一貫性を確認する．
- **処理 c**：検証者はタイムスタンプを発行者に送り，発行者が，そのタイムスタンプと自分が保管するデータとの整合性を確認し，確認結果を検証者に通知する．T がタイムスタンプを構成するデータでない場合には，発行者は T も検証者に送る．

表 1　10 のグループと各グループに適用可能な検証手続

グループ	分類の観点			各グループに適用可能な検証手続
	ﾀｲﾑｽﾀﾝﾌﾟに含まれるﾃﾞｰﾀ	E_{TSI} の取得可能性	ﾀｲﾑｽﾀﾝﾌﾟの生成方法	
NN-U-I	NN	U	I	**ac, abc**
NN-U-L			L	**ac, abc**
NN-A-I		A	I	**ac, abc, acd, abcd, acde, abcde**
NN-A-L			L	**ac, abc, acd, abcd, acde, acdf, abcde, abcdf, acdef, abcdef**
TN-U-I	TN	U	I	**a, ab, ac, abc**
TN-U-L			L	**a, ab, ac, abc**
TN-A-I		A	I	**a, ab, ac, ad, abc, abd, acd, ade, abcd, abde, acde, abcde**
TN-A-L			L	**a, ab, ac, ad, abc, abd, acd, ade, adf, abcd, abde, abdf, acde, acdf, adef, abcde, abcdf, abdef, acdef, abcdef**
TE-A-I	TE	A	I	**a, ab, ac, ad, ae, abc, abd, abe, acd, ace, ade, abcd, abce, abde, acde, abcde**
TE-A-L			L	**a, ab, ac, ad, ae, af, abc, abd, abe, abf, acd, ace, acf, ade, adf, aef, abcd, abce, abcf, abde, abdf, abef, acde, acdf, acef, adef, abcde, abcdf, abcef, abdef, acdef, abcdef**

表 2　3 つのケースにおいて実行可能な検証処理

タイムスタンプ方式	実行可能な検証処理						
	ケース 1（検証者がデータを入手不可能なエンティティ）			ケース 2（検証者がデータを入手不可能なエンティティ）			ケース 3
	発行者	証拠補強者	発行依頼者	発行者と証拠補強者	発行者と発行依頼者	証拠補強者と発行依頼者	
NN	（T を入手不可能）	a, b, c, d, f	a, b, c, d, e	（T を入手不可能）		a, b, c, d	（T を入手不可能）
TN	a, b			a, b			a, b
TE	a, b, d, e, f			a, b, d, f	a, b, d, e		a, b, d

・**処理 d**：検証者は，発行者から得る E_{TSI} を用いて，タイムスタンプと発行者のデータベースのデータとの整合性を確認する．
・**処理 e**：検証者は，証拠補強者から得る E_{AMP} を用いて E_{TSI} の一貫性を確認する．
・**処理 f**：検証者は，発行依頼者から得る E_{ORE} を用いて E_{TSI} の一貫性を確認する．

処理 **a** は，M とタイムスタンプの対応関係を確認するものであり，必須の処理となる．したがって，5 種類の処理 **b**～**f** の組み合わせによって 32 通りの検証手続が想定される．以下では，処理を表すアルファベットを並べて検証手続を示す．例えば，**ade** は 3 つの処理 **a**，**d**，**e** を実行する検証手続を表す．

2.6 タイムスタンプ方式の分類

タイムスタンプ構成データの種類，検証者による E_{TSI} の入手可能性，タイムスタンプの生成方法の観点から，タイムスタンプ方式を分類する．

第一に，タイムスタンプが T と E_{TSI} を含まない時刻・証拠無方式（NN，No time information and No evidence），T を含むが E_{TSI} を含まない時刻付・証拠無方式（TN，Time information and No evidence），T と E_{TSI} の両方を含む時刻・証拠付方式（TE，Time information and Evidence）に分類する．

第二に，検証者が E_{TSI} を取得可能な取得型方式（A，evidence-Available scheme）と，E_{TSI} を取得不可能な非取得型方式（U，evidence-Unavailable scheme）に分類する．

第三に，他のタイムスタンプを構成するデータを用いて生成する連鎖型方式（L，Linked time stamp scheme）と，他のタイムスタンプを構成するデータを用いずに生成する個別型方式（I，Isolated time stamp scheme）に分類する．これらの観点から，タイムスタンプ方式を NN-U-I，NN-U-L，NN-A-I，NN-A-L，TN-U-I，TN-U-L，TN-A-I，TN-A-L，TE-A-I，TE-A-L の 10 のグループに分類する（表 1 参照）．

次に，各グループに適用可能な検証手続を調べる．処理 **a** はすべてのグループの検証手続に必須である．処理 **b** はすべてのグループの検証手続に適用できる．処理 **c** は，時刻・証拠無方式のグループで，T を入手する必要があるため必須であり，それ以外では必須ではないが適用できる．処理 **d**，**e**，**f** は，非取得型方式のグループでは，検証者が E_{TSI} を入手不可能なため適用できない．処理 **f** は連鎖型方式のグループにのみ適用できる．このようにして各グループで適用可能な検証手続を整理すると，108 の方式に分類される．

なお，同一の検証手続を用いるタイムスタンプの集合をタイプと定義する．例えば，検証手続 **abde** を用いる方式の集合を「タイプ **abde**」と呼ぶ．

3　検証手続の可用性の尺度

3.1　宇根・松本[9]の検討結果

宇根・松本[9]は，タイムスタンプ方式の可用性を

次の 2 つを満足する特性と定義している．

- **発行依頼者が，既定の期間内において，既定の手続に沿って，既定の時間内に発行者から適正なタイムスタンプの発行を受けることができ，証拠補強者を利用する方式の場合には，証拠補強者が発行者から既定の時間内に適正な E_{AMP} を得ることができる（発行手続の可用性）．**
- **検証者が，既定の期間内において，既定の手続に沿って，発行者等のエンティティから適正なデータを入手し，既定の時間内にタイムスタンプを検証することができる（検証手続の可用性）．**

宇根・松本[9]は，発行・検証手続の可用性が損なわれる場合を整理し，そのような場合に各方式間で発行・検証手続への影響がどのように異なるかを検討した．その結果，発行手続に関しては，処理 **e** を含む検証手続を用いる方式では，処理 **e** を用いない方式に比べて発行手続が正常に完了しない場合が多いことを示した．一方，検証手続に関しては，検証者が他のエンティティから検証に用いるデータを入手できない場合を，発行者，証拠補強者，E_{ORE} を有する発行依頼者のいずれか 1 つのエンティティから入手できない場合（ケース 1），いずれか 2 つのエンティティから入手できない場合（ケース 2），3 つのエンティティすべてから入手できない場合（ケース 3）に分類した上で，各ケースにおいて実行可能な検証処理を整理した（表 2 参照）．

3.2 発行手続と検証手続の可用性

本稿では，宇根・松本[9]に基づき，発行手続および検証手続の可用性の観点からタイムスタンプ方式を分類する際にどのような尺度を利用することが適当かを検討する．

まず，具体的にどのような観点からタイムスタンプ方式を分類するかを考える．発行手続に関しては，検証手続に処理 **e** が含まれるか否かによって異なることを宇根・松本[9]が示している．すなわち，処理 **e** を含む検証手続を用いる方式では，証拠補強者が E_{AMP} を発行者から入手できない場合に発行手続が正常に完了しない反面，処理 **e** を含まない検証手続を用いる方式では，証拠補強者を利用しないため，このような問題は発生しない．しかし，処理 **e** を含む検証手続を用いる主な方式である Cuculus[2]や TIMESEC[6]等では，E_{AMP} を数日後に公表する等，証拠補強者や発行者によるリアルタイムでのデータ処理が要求されておらず，証拠補強者が E_{AMP} を発行者から入手できない状況が発生する可能性は非常に小さいと考えられる．こうした現状を踏まえると，発行手続の可用性に関してタイムスタンプ方式間で実際に差異が生じる可能性は小さいと考えられるため，発行手続の可用性が損なわれる状況は検討対象外とする．

一方，検証手続に関しては，検証者が他のエンティティからデータを入手できない状況（ケース 1〜3）において実行可能な検証処理がタイムスタンプ方式の種類によって異なることが宇根・松本[9]によって示されている．そこで，検証手続の可用性の観点からタイムスタンプ方式を分類し，実行可能な検証処理に着目して分類を行うこととする．

3.3 検証手続と検証処理の関係

こうした方針でタイムスタンプ方式の分類方法について検討を行うためには，検証手続と検証処理の関係を整理しておくことが必要である．検証手続と検証処理の関係として，「検証処理が 1 つでも実行不可能となった場合には，検証手続全体が無意味となる」とする立場と，「一部の検証処理が実行不可能な場合でも，実行可能な検証処理が残っていれば，検証手続全体が無意味となることはない」とする立場が考えられる．

これらのうちどちらを採用するかによって，検証手続の可用性に関する検討の結果は異なる．「検証処理が 1 つでも実行不可能になると，検証手続全体が無意味となる」と考える場合，分類結果は極めて単純になる．すなわち，すべての方式は，問題が発生しても検証手続の可用性が確保される方式と，検証手続の可用性が完全に失われる方式のいずれかに分類されることとなる．これに対して，「実行可能な検証処理が残っていれば，検証手続全体が無意味となることはない」と考える場合，可用性が確保されるか，もしくは，完全に失われるかという二分法ではなく，「ある問題が発生した際にどの検証処理が実行可能か」という観点でタイムスタンプ方式を詳細に分類・比較することが可能となる．

また，ここで，「実行可能な検証処理が残っていれば，検証手続全体が無意味となることはない」との立場を採った場合，実行可能な検証処理に基いて，「検証者が他のエンティティからデータを入手できないといった事態に陥ると，タイムスタンプの安全性にどのような影響が及ぶか」といった方向へ議論を比較的容易に発展させることができる．これは，Une and Matsumoto[10]において，タイムスタンプの改ざん攻撃に対する安全性が検証手続に依存することが示されていることによる．タイムスタンプ方式の安全性につながる議論は，タイムスタンプ方式の安全性評価を行うタイムスタンプ方式の利用者にとって有用であると考えられる．

さらに，実際のタイムスタンプのサービスにおいて一部の検証処理が実行不可能となった場合を想定すると，不完全ではあるものの，実行可能な検証処理によってタイムスタンプの検証を行い，その結果を基に，検証者がタイムスタンプの証明内容に関して判断を下すことになると考える方が自然である．

このように，利用者に対する有用性や，一部の検証処理が実行不可能となった場合に想定される実際の対応を考慮すると，「一部の検証処理が実行不可能でも，実行可能な検証処理が残っていれば，検証

手続全体が無意味となることはない」との考え方を採用することが有用であると考えられる．本稿では，こうした考え方を採用した上で，「検証者が他のエンティティからデータを入手できない場合に実行可能な検証処理がどれだけ残っているか」，すなわち，実行可能な検証処理の数に焦点を当てて，タイムスタンプ方式の分類方法を検討する．

3.4 検証処理数の割合と絶対数

実行可能な検証処理の数に基づいてタイムスタンプ方式の分類・比較を行う場合，既定の検証処理数に占める実行可能な検証処理数の割合を尺度とする方法と，実行可能な検証処理数の絶対数を尺度とする方法，の 2 つが考えられる．

これらのうち，既定の検証処理数に占める実行可能な検証処理数の割合を尺度とすると，タイムスタンプ方式によって既定の検証処理数が異なるため，本稿で前提としている検討方針と整合的な結果が得られない場合がある．そうした例の 1 つとして，検証者が発行者からデータを入手できない場合において TN-A-I-**abc** と TN-A-I-**abcde** を比較するケースを考える．表 2 から，TN-A-I-**abc** と TN-A-I-**abcde** における既定の検証処理数（それぞれ 3，5）に占める実行可能な検証処理（ともに処理 **a** と処理 **b**）の数（ともに 2）の割合はそれぞれ 2/3，2/5 となる．これは，TN-A-I-**abc** が検証手続の可用性の観点で相対的に望ましいことを意味している．しかし，3.3 で説明したように，本稿では「ある問題が発生した際にどの検証処理が実行可能か」という観点で検証手続の可用性を検討しており，両者の実行可能な検証手続は同一であることから，検証者が発行者からデータを入手できない場合における両者の検証手続の可用性は同等と判断することが妥当である．したがって，既定の検証処理に占める実行可能な検証処理数の割合を尺度としたときに，本稿における検討の方針と整合的な結果が得られないこととなる．一方，実行可能な検証処理数の絶対数を尺度として用いる場合，このような問題が発生しない．

そこで，本稿では，ケース 1〜3 における実行可能な検証処理数の絶対数（以下，実行可能な検証処理数という）を尺度としてタイムスタンプ方式の分類・比較を行うこととする．

4 検証手続の可用性による分類

4.1 各ケースにおいて実行可能な検証処理数

まず，ケース 1 では，検証者がデータを入手できないエンティティとして発行者，証拠補強者，発行依頼者の 3 通りが想定され，それぞれの場合において実行可能な検証処理数が異なる場合も考えられる．このような場合，各方式において検証手続の可用性が最も損なわれる状況を基準として各方式を分類・比較することとする．具体的には，実行可能な検証処理数が複数存在する場合，その中でも最小のものをケース 1 における実行可能な検証処理数とする．例として，TN-A-I-**abde** におけるケース 1 の実行可能な検証処理数を調べる．検証者が発行者からデータを入手できない場合，実行可能な検証処理は処理 **a**, **b** であり，検証処理数は 2 となる．一方，証拠補強者からデータを入手できない場合，実行可能な検証処理は処理 **a**，**b**，**d** であり，検証処理数は 3 となる．このため，TN-A-I-**abde** におけるケース 1 の実行可能な検証処理数は，3 と 2 を比較して相対的に小さい 2 となる．

ケース 2 では，検証者がデータを入手できないエンティティとして，発行者と証拠補強者，発行者と発行依頼者，証拠補強者と発行依頼者の 3 通りが想定され，各場合で実行可能な検証処理数が異なることも考えられる．これらについても，ケース 1 と同様，最小のものを実行可能な検証処理数とする．

以上の要領で各方式における実行可能な検証処理数を調べる．ケース 1〜3 における実行可能な検証処理数がそれぞれ 5，4，3 となる方式の集合の場合，その集合を(5, 4, 3)と表わすこととする．括弧内の第 1〜3 要素がそれぞれケース 1〜3 の実行可能な検証処理数を表わす．なお，検証者が日時データ T を入手することができず，実行可能な検証処理が存在しない場合，“ N ”（Nonsense）という記号を用いて表わす．この結果，タイムスタンプ方式は，(5, 4, 3)，(4, 3, 3)，(4, 3, 2)，(3, 3, 3)，(3, 2, 2)，(3, 2, 1)，(2, 2, 2)，(2, 1, 1)，(1, 1, 1)，(N, N, N)の 10 の集合に分類される（表 3 参照）．

表 3　実行可能な検証処理数による タイムスタンプ方式の分類

分類	タイムスタンプ方式
(5, 4, 3**)**	TE-A-L-**abcdef**
(4, 3, 3**)**	TE-A-**abcde** TE-A-L-**abcdf**, **abdef**
(4, 3, 2)	TE-A-L-**acdef**, **abcef**
(3, 3, 3)	TE-A-**abd**, **abcd**, **abde** TE-A-L-**abdf**
(3, 2, 2)	TE-A-**abce**, **acde** TE-A-L-**abcf**, **acdf**, **abef**, **adef**
(3, 2, 1)	TE-A-L-**acef**
(2, 2, 2)	TN-**ab**, **abc** TN-A-**abd**, **abcd**, **abde**, **abcde** TN-A-L-**abf**, **adf**, **abdf**, **abcdf**, **abdef**, **abcdef** TE-A-**ab**, **ad**, **abc**, **acd**, **ade**, **abe** TE-A-L-**abf**, **adf**
(2, 1, 1)	TE-A-**ace** TE-A-L-**acf**, **aef**
(1, 1, 1)	TN-**a**, **ac**, TN-A-**ad**, **acd**, **ade**, **acde** TN-A-L-**adf**, **acdf**, **adef**, **acdef** TE-A-**a**, **ac**, **ae**, TE-A-L-**af**
(N, N, N)	NN

（注） 例えば，(5, 4, 3**) は，ケース** 1〜3 **での実行可能な検証手続数がそれぞれ** 5, 4, 3 **であることを意味する．**

表 4　既存の方式への適用結果

タイムスタンプ方式	グループ・タイプ	実行可能な検証処理		検証手続の可用性による分類
		ケース 1	ケース 2, 3	
電子公証制度	TN-U-I **-ab**	**a, b**		(2, 2, 2)
時刻署名分散システム				
Digital Notary /SecureSeal	TN-U-L **-ac**	**a**		(1, 1, 1)
Benaloh **と** de Mare **の** **プロトコル**	TE-A-L **-ad**	**a, d**		(2, 2, 2)
PKITS	TN-A-L **-abde**	・**a, b***	**a, b**	
TIMESEC		・**a, b, d****		
Cuculus	TE-A-L **-abde**	・**a, b, d, e*** ・**a, b, d****	**a, b, d**	(3, 3, 3)

（注）*と**は，検証者がデータを発行者と証拠補強者からそれぞれ入手できない場合に実行可能な検証手続を示す.

4.2 主要な方式への検討結果の適用

主なタイムスタンプ方式として，電子公証制度[4], 時刻署名分散システム[8]，Digital Notary[7]/SecureSeal[5]，Benaloh と de Mare のプロトコル[1]，PKITS[3]，TIMESEC[6]，Cuculus[2]を取り上げ，各ケースにおける実行可能な検証処理，および，各方式が表 3 で分類された集合のいずれに属するかを検討する（表 4 参照）.

まず，TN-U-I-**ab** に分類される電子公証制度と時刻署名分散システムでは, ケース 1〜3 において実行可能な検証処理は既定の検証処理と同様に **a** と **b** となり，(2, 2, 2)に属する．TE-A-L-**ad** に分類される Benaloh と de Mare のプロトコルは，ケース 1〜3 で実行可能な検証処理が既定の検証処理と同様に **a** と **d** となり，(2, 2, 2)に属する．TN-U-L-**ac** に分類される Digital Notary/SecureSeal は, ケース 1〜3 で実行可能な検証処理が **a** のみであり，(1, 1, 1)に属する．TN-A-L-**abde** に分類される PKITS と TIMESEC は, ケース 1 の中でも検証者が発行者からデータを入手できない場合に実行可能な検証処理は **a** と **b** であり，証拠補強者からデータを入手できない場合に実行可能な検証処理は **a**，**b**，**d** となる．また，ケース 2，3 において実行可能な検証処理は **a**，**b** となる．この結果，PKITS と TIMSEC は(2, 2, 2)に属する．最後に，Cuculus は，ケース 1 の中でも検証者が発行者からデータを入手できない場合に実行可能な検証処理は **a**，**b**，**d**，**e** であり，証拠補強者からデータを入手できない場合に実行可能な検証処理は **a**，**b**，**d** である．また，ケース 2，3 において実行可能な検証処理は **a**，**b**，**d** である．この結果，Cuculus は(3, 3, 3)に属する．

5　おわりに

本稿では，可用性の観点からタイムスタンプ方式を分類・比較する際に，検証者が他のエンティティから検証に用いるデータを入手できない場合に実行可能な検証処理数を尺度として用いることが有用であることを示した．その上で，実行可能な検証処理によってタイムスタンプ方式が 10 の集合に分類されることを示し，7 つの既存のタイムスタンプ方式における検証手続の可用性上の特徴を明らかにした.

今後は，可用性に加え，Une and Matsumoto[10]を参考にしながら安全性やコストも考慮してタイムスタンプ方式の評価を行う方法を検討する方針である.

参考文献

[1]Benaloh, J. and M. de Mare, “One-Way Accumulators: A Decentralized Alternative to Digital Signature,” *Pro- ceedings of EUROCRYPT ‘93*, LNCS 765, pp. 274-285, Springer-Verlag, 1994.

[2]Cybernetica, “Cuculus: How does it work?” (http://www. cyber.ee/research/cuculus.html, access: March 27, 2002).

[3]Fabrica Nacional de Moneda y Timbre, *PKITS: Deliverable D4a Description and Results of the Unstructured Data Time-Stamping Protocol Implementation*, Revision Number 16, July 30, 1998.

[4]法務省民事局, “ 電子取引法制に関する研究会報告書, ” 1998 年 3 月.

[5]NTT データ, “SecureSeal＜テクニカル情報＞,” (http:// 210.144.76.11/, access: March 27, 2002).

[6]Preneel, B., B. V. Rompay, J.-J. Quisquater, H. Massias and J. S. Avila, “Design of a timestamping system,” *TIMESEC Technical Report WP3*, 1998 (http://www.dice.ucl.ac.be/crypto/TIMESEC/TR3.ps.gz).

[7]Surety.com, “Secure Time/Data Stamping in a Public Key Infrastructure,” (http://www.surety.com/home/pki.pdf, access: March 27, 2002).

[8]Takura, A., S. Ono and S. Naito, “Secure and Trusted Time Stamping Authority,” *Proceedings of IWS’99*, pp.123-128, Springer-Verlag, 1999.

[9]宇根正志，松本勉, “ タイムスタンプ方式に対する可用性の定義と評価, ”『コンピュータセキュリティシンポジウム 2001 予稿集』, pp.79-84, 情報処理学会，2001 年 10 月.

[10]Une, M. and T. Matsumoto, “ A Framework to Evaluate Security and Cost of Time Stamping Schemes, ” *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E85-A, No. 1, pp.125-139, Jan. 2002.