可用性および安全性の観点からみた各タイムスタンプ方式間の関係

宇根正志[†,††] 松本勉[†,†††]

タイムスタンプ技術は，特定のデータが特定日時に存在したことを証明する技術である．最近では，電子商取引の拡大等にともなって様々なタイムスタンプ方式が提案されており，タイムスタンプの安全性確保や長期間安定したサービス提供の実現が重要な検討課題となっている．こうした背景から，タイムスタンプ方式のセキュリティ評価に関する様々な研究がこれまでに行われているものの，タイムスタンプ方式に対する可用性についての体系的な研究については皆無に近く，タイムスタンプ方式に対する可用性評価の研究が必要とされている．本稿では，可用性および安全性の両面からタイムスタンプ方式について検討する．まず，タイムスタンプ方式に対する可用性を定義し，タイムスタンプの発行・検証手続において可用性が損なわれるケースを示す．次に，可用性および安全性の観点からタイムスタンプ方式を 37 のカテゴリに分類したうえで，各カテゴリ間の関係を明らかにする．最後に，本検討結果を既存の 7 つのタイムスタンプ方式に適用する．

Relationships between Time Stamping Schemes from Viewpoints of Availability and Integrity

Masashi Une[†,††] and Tsutomu Matsumoto[†,†††]

Time stamping is a technique used to prove the existence of certain digital data prior to a specific point in time. With the recent expansion of electronic commerce, various time stamping schemes have been proposed, and it is important to discuss how to ensure the integrity of a time stamp and how to steadily provide time stamping services for a long time. While many studies have been made on the security evaluation of time stamping schemes, few studies have focused on their availability. It is necessary to study the availability evaluation of time stamping schemes. This paper discusses time stamping schemes from the following two viewpoints: the availability of time stamping schemes and the integrity of time stamps. First, we define the availability of time stamping schemes and clarify cases in which the availability of the issuing and verification procedures is spoiled. Secondly, we classify the schemes into thirty-seven categories from both the availability and the integrity and discuss the relationships between the categories. Finally, we apply our results to seven existing schemes.

1. はじめに

タイムスタンプ技術は，特定のデータが特定日時に存在したことを証明する技術である．近年の電子商取引や電子文書管理の利用拡大等にともなって各種タイムスタンプ方式が提案されており，わが国では SecureSeal[9] 等の商用サービスが開始されている．また，標準化の分野では，IETF や ISO がタイムスタンプ・サービスの標準化を進めているところである[1),8)]．

こうした中，タイムスタンプ方式におけるセキュリティの確保が重要な課題となっており，タイムスタンプ方式の体系的な安全性評価に関する研究が進められている．まず，宇根・松本は，文献 13) において，既存の代表的なタイムスタンプ方式である Cuculus[4] と PKITS[5] を取り上げ，これらの方式におけるタイムスタンプの改ざん攻撃に対する安全性に関して，具体的な仕様を考慮したうえで検討を行った．また，宇根・松本は，文献 14)，15) において，タイムスタンプを定義したうえで，タイムスタンプ方式の分類方法を提案し，タイムスタンプ方式を評価するための枠組みを示した．これらの研究を土台として，宇根・松本は，文献 16) において，各方式ごとにタイムスタンプの改ざん攻撃に対する安全性を検討したうえで，タイムスタンプ方式を 10 種類に分類し，各タイムスタンプ

† 横浜国立大学大学院工学研究科
Graduate School of Engineering, Yokohama National University
†† 日本銀行金融研究所
Institute for Monetary and Economic Studies, Bank of Japan
††† 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University

方式間の関係を明らかにした．文献 13) から文献 16) までのタイムスタンプ方式の評価に関する一連の研究は，文献 18) においてまとめられている．

ただし，実際にタイムスタンプ方式の利用を検討する場合，安全性の評価だけではなく，可用性の評価が必要である．タイムスタンプ技術は，データがある時点に存在したことを長期間証明することが求められるアプリケーションを対象としており，タイムスタンプ・サービスの提供者が廃業したとしても，既存のタイムスタンプを検証できることが必要とされる．また，多くのタイムスタンプ方式では，利用者がオンラインでタイムスタンプの発行・検証をサービス提供者に要求する形態が採用されており，サービス提供者がサービス妨害攻撃（Denial-of-Service Attack）等の標的となった場合でも検証手続を実行できるようにしておくことも重要である．このように，各種タイムスタンプ方式が可用性の観点でどのような性質を有しているかを検討することは，具体的なタイムスタンプ方式を設計したり，タイムスタンプ・サービスの利用を検討したりする際に有用である．

タイムスタンプ方式に対する可用性に関して体系的に検討した研究として，文献 17) があげられる．文献 17) は，タイムスタンプ方式に対する可用性を定義し，タイムスタンプの発行・検証手続において可用性が損なわれるケースを整理したほか，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どの検証処理が実行可能かについて検討を行った．

本稿では，文献 17), 18) の検討結果をベースに，可用性と安全性の両方の観点からタイムスタンプ方式について検討を行う．まず，可用性の観点から，検証者が各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どの検証処理が実行可能かを検討したうえで，各方式間の関係について検討する．次に，タイムスタンプの改ざん攻撃に対する安全性についての検討結果[18] をふまえ，可用性と安全性の両面からタイムスタンプ方式を 37 種類に分類し，各カテゴリ間の関係を改めて検討する．最後に，これらの検討結果を既存のタイムスタンプ方式に適用する．

本稿の構成は次のとおりである．まず，2 章では，検討の前提となるタイムスタンプ方式の枠組みを説明し，3 章ではタイムスタンプ方式に対する可用性の定義，および，可用性が損なわれるケースについて説明し，本稿における検討の内容を説明する．4 章では，検証者が各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を検討したうえで，可用性の観点からタイムスタンプ方式を分類し，各方式間の関係を明らかにする．5 章では，安全性と実行可能な検証処理数の両方の観点からタイムスタンプ方式を分類し，各方式間の関係を示す．6 章では，既存の 7 つのタイムスタンプ方式に本検討結果を適用する．最後に，7 章で検討結果をまとめ，今後の課題を示す．

2. タイムスタンプ方式の枠組み

2.1 エンティティ

まず，タイムスタンプ方式を構成する 5 つのエンティティを説明する[14]．

- **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 つの発行者と見なす．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り，“*TSI*” は “Time Stamp Issuer” を意味する．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られる．“*AMP*” は “AMPlifier” を意味する．
- **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 T の時点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} を安全に保管することで E_{TSI} の証拠性を補強する役割を持つ．
- **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り，検証対象のタイムスタンプとは別のタイムスタンプに含まれる．“*ORE*” は “Other REquester” を意味する．
- **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

まず，タイムスタンプを，「特定のデータ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

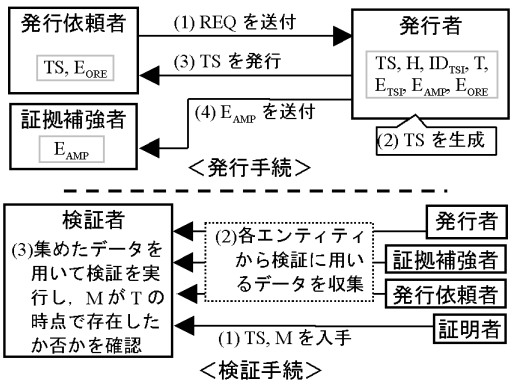

図 1 タイムスタンプの発行・検証手続
Fig. 1 Issuing and verification procedures of a time stamp.

とも H と ID_{TSI} を含むデータ」と定義する．ただし，タイムスタンプの対象となるデータを M，そのハッシュ値を H，発行者の識別データを ID_{TSI} とする．また，E_{TSI} と E_{ORE} のほか，以下で説明する T，$Info_{INT}$，ID_{REQ}，ID_{AMP}，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．たとえば，$Info_{INT}$ の一形態としてディジタル署名が考えられる．
- 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タイムスタンプを送付．
(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．
- **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** の組合せによって 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．たとえば，**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} の取得可能性，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 1 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．なお，E_{TSI} を含むが T を含まない方式も考えられるが，そのような方式は実際に利用されるとは考えにくいことから検討対象外とする．E_{TSI} を含むタイムスタンプの意義は，検証者が発行者から追加的にデータを入手することなく検証処理 **d** を実行できる点にあると考えられる．しかし，E_{TSI} を含むが T を含まないタイムスタンプを利用する場合には，検証者は検証処理 **d** を実行する際に発行者から追加的に T を入手する必要があり，E_{TSI} をタイムスタンプに含める意義が失われる．このため，E_{TSI} を含み T を含まないタイムスタンプが実際に利用されるとは考えにくく，本稿では想定しないこととした．ちなみに，これまでに時刻・

表 1 10 のグループと各グループに適用可能な検証手続
Table 1 Ten groups of time stamping schemes and applicable verification procedures.

グループ	分類の観点			各グループに適用可能な検証手続
	タイムススタンプに含まれるデータ	E_{TSI} の取得可能性	タイムスタンプの生成方法	
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**

証拠無方式，時刻付・証拠無方式，時刻・証拠付方式に関してはいくつかの具体的な方式が提案されているものの，E_{TSI} を含み T を含まないタイムスタンプを用いる方式に関しては，筆者の知る限り具体的な方式は提案されていない．第 2 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 3 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使わずに生成する個別型方式（I，Isolated time stamp scheme）に分類する．タイムスタンプ方式は 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 のグループに分類される（**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可能である．処理 **c** は，時刻・証拠無方式のグループにおいて，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なく適用可能である．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不可能である．処理 **f** は連鎖型方式のグループにのみ適用可能である．これらをもとに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（表 1 参照）．

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．たとえば，検証手続 **abde** を用いる方式の集合を「タイプ**abde**」と呼ぶ．

3. タイムスタンプ方式に対する可用性

3.1 可用性の定義

情報システムの可用性（availability）の一般的な定義としては，情報セキュリティ管理の指針 ISO/IEC TR 13335（GMITS）[7] において，「あらかじめ権限を付与されたエンティティが（情報システムに）アクセス可能であり，利用可能である，という特性」と定義されている．タイムスタンプ方式では，「エンティティ」には発行依頼者と検証者が該当するほか，「アクセスする」または「利用する」という行為は，発行依頼者の場合，タイムスタンプの発行を発行者に依頼し，タイムスタンプを得るとともに，検証手続に証拠補強者を利用する場合には，証拠補強者が発行者から検証に用いるデータ E_{AMP} を得ることに対応する．一方，検証者の場合，タイムスタンプを検証することに対応する．ただし，発行・検証手続が完了するまでに予想外に長い時間がかかる場合にはサービスとして意味をなさないケースもあり，既定の時間内にサービスが完了することが必要であると考えられる．

これらをふまえ，タイムスタンプ方式に対する可用性を，次の 2 つを満足する特性と定義する．

- 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）．

3.2 発行手続の可用性

どのような場合にタイムスタンプの発行・検証手続の可用性が損なわれるかを検討する．発行手続の可用性が損なわれる主なケースとして，次の 9 つがあげられる．

(1) 発行依頼者は，タイムスタンプ発行要求データ *REQ* を既定の時間内に発行者に発信できない．
(2) 発行依頼者が *REQ* を発信した後，既定の時間内に *REQ* が発行者に到達しない．
(3) 発行依頼者が *REQ* を発信した後，発行者のデータ処理機能の問題から，発行者が既定の時間内に *REQ* を受信できない．
(4) 発行者は，*REQ* を受信した後，既定の時間内に適正なタイムスタンプを生成・発信できない．
(5) 発行者が *TS* を発信した後，既定の時間内にタイムスタンプが発行依頼者に到達しない．
(6) 発行者がタイムスタンプを発信した後，発行依頼者のデータ処理機能の問題から，発行依頼者が既定の時間内にタイムスタンプを受信できない．
(7) 発行者が証拠補強者に対して既定の時間内に E_{AMP} を発信できない．
(8) 発行者が E_{AMP} を発信した後，既定の時間内に E_{AMP} が証拠補強者に到達しない．
(9) 発行者が E_{AMP} を発信した後，証拠補強者のデータ処理機能の問題から，証拠補強者が既定の時間内に E_{AMP} を受信できない．

上記 (1)，(6) は発行依頼者のデータ処理機能に問題が生じた場合に発生し，(3)，(4)，(7) は発行者のデータ処理機能に問題が生じた場合に発生する．(9) は証拠補強者のデータ処理機能に問題が生じた場合に発生する．一方，(2)，(5)，(8) は各エンティティ間のネットワークの遅延や不通等の問題が生じた場合に発生する．これらのうち，(1)〜(6) のいずれかが発生すると，どの方式においても発行手続は正常に完了せず，発行手続の可用性が喪失する．

(7)〜(9) は，処理 **e** を含む検証手続を用いる方式で問題となる．このような方式では，(7)〜(9) によって証拠補強者が E_{AMP} を入手できない場合，発行手続が正常に完了しない．ただし，処理 **e** を含む検証手続を用いる主な方式として Cuculus [4] や TIMESEC [10] 等があげられるが，これらの方式では，E_{AMP} を数日後に公表する等，発行者から証拠補強者へのデータ送信や各種処理等をリアルタイムで実行することが必ずしも必要となっていない．このため，リアルタイムでの処理の可否が問題となる (1)〜(6) に比べて，(7)〜(9) が発生する可能性は非常に小さいと考えられる．一方，処理 **e** を含む検証手続を用いない方式では，これらは問題とならない．

3.3 検証手続の可用性

検証手続の可用性が損なわれる主なケースとして，次の 7 つがあげられる．

(1) 検証者は，検証に用いるデータの送信を要求するデータ *REQ'* を，既定の時間内に各エンティティに発信できない．
(2) 検証者が *REQ'* を発信した後，*REQ'* が各エンティティに既定の時間内に到達しない．
(3) 検証者が *REQ'* を発信した後，各エンティティのデータ処理機能の問題から，既定の時間内に各エンティティが *REQ'* を受信できない．
(4) 各エンティティは，*REQ'* を受信した後，要求された適正なデータを既定の時間内に検証者に発信できない．
(5) 各エンティティがデータを発信した後，既定の時間内にデータが検証者に到達しない．
(6) 各エンティティがデータを発信した後，検証者のデータ処理機能の問題から，既定の時間内に検証者がデータを受信できない．
(7) 検証者は，入手した各種データを用いて，タイムスタンプを検証するための既定の各種演算を，既定の時間内に実行できない．

上記 (1)，(6)，(7) は検証者のデータ処理機能に問題が生じた場合に発生し，(3)，(4) は検証者にデータを提供する各エンティティのデータ処理機能に問題が生じた場合に発生する．たとえば，発行者が廃業し，その機能を継続不可能な場合もこれらに含まれる．また，(2)，(5) は各エンティティ間のネットワークに大幅な遅延や不通等の問題が生じた場合に発生する．

このように，(1)〜(6) が生じた場合，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する方式では，検証者がそれらのデータを入手できなくなり，検証手続が正常に完了しない．

3.4 可用性に関する検討の範囲

タイムスタンプ方式に対する可用性の検討として，次の 2 つが考えられる．

第 1 は，3.2 節と 3.3 節で説明した各問題が発生する可能性がどの程度かを検討するというものである．各問題が発生する可能性は，各方式で利用されているエンティティやネットワークの属性等に依存する．たとえば，二重化等によって発行者のデータ処理機能の信頼性を高めるとか，複数の発行者が協力してタイムスタンプを発行する仕組みを採用する，といった手段

が講じられる場合には，3.2 節と 3.3 節の各問題が発生する可能性は低下すると考えられる．これらの各問題が発生する可能性を検討するためには，各種タイムスタンプ方式においてどのような対策が講じられているかを個別に吟味する必要がある．

第 2 は，3.2 節や 3.3 節の各問題が発生したという前提の下で，タイムスタンプの発行・検証手続がどの程度実行可能かを検討するというものである．各問題が発生した場合にどの発行・検証処理が実行可能かは，各方式の発行・検証手続の種類やタイムスタンプの形態等に依存すると考えられる．たとえば，検証に用いられるデータがタイムスタンプに含まれる方式では，検証者が他のエンティティからデータを入手できなくても検証手続を実行できる可能性がある．

これらのうち，本稿では第 2 の検討に焦点を当てる．第 1 の検討に関しては，本稿では各タイムスタンプ方式の詳細な仕様に立ち入らずに検討を行うことを目標としていることから，ここでは取り上げない．

次に，3.2 節と 3.3 節の各問題のうち，どの問題の発生を前提に検討を進めるかを考える．まず，3.2 節の (1)〜(6) が生じると，どの方式においても発行者がタイムスタンプを入手できないほか，3.3 節の (7) が生じると，どの方式においても検証者は検証手続を実行できず，異なるタイムスタンプ方式の間で可用性に差が生じない．このため，これらの問題の発生は検討対象外とする．また，3.2 節の (7)〜(9) が発生する可能性は非常に小さいと考えられることから，3.2 節の (7)〜(9) も検討対象外とする．これらに基づき，3.3 節の (1)〜(6) が生じ，検証者が各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，各タイムスタンプ方式における検証手続の可用性にどのような差異が生じるかを検討する．

ここで，検証手続の可用性を検討する際に，検証手続と検証処理の関係をどのように考えるかが問題となる．すなわち，「検証手続を構成する検証処理はそれぞれ独立しておらず，検証処理が 1 つでも実行不可能となった場合には，検証手続の可用性が完全に失われる」と考える場合と，「検証手続を構成する検証処理はそれぞれ独立しており，一部の検証処理が実行不可能となった場合でも，残りの検証処理が実行可能であれば，検証手続の可用性は部分的に確保される」と考える場合とでは，検証手続の可用性の検討結果が異なる．「検証処理がそれぞれ独立していない」と考える場合，ある方式における検証手続の可用性の検討結果は，「ある問題が発生しても可用性が確保される」もしくは「ある問題が発生すると可用性が完全に失われる」のいずれかのみとなる．これに対して，「検証処理はそれぞれ独立している」と考える場合，ある問題が発生した際に，検証手続を構成する検証処理の中でどの検証処理が引き続き実行可能かを明らかにすることができる．タイムスタンプ方式の利用者がどの方式を選ぶかを検討する際に，「発行者からデータを入手できないといった事態に陥った場合，実際にどのような検証処理が実行可能か」，また，「その結果，タイムスタンプの安全性にどのような影響が及ぶか」といった情報は有用であると考えられる．このため，本稿では，タイムスタンプ方式の利用者に対する有用性を考慮して「検証処理はそれぞれ独立している」との考え方を採用し，実行可能な検証処理に着目して検討を進めることとする．

4. 実行可能な検証処理数とそれに基づく方式の分類

4.1 3 つのケース

検証者が検証に用いるデータを入手できない場合として，次の 3 つのケースが想定される．

- **ケース 1**：検証者が，いずれか 1 つ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．
- **ケース 2**：検証者が，いずれか 2 つ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．
- **ケース 3**：検証者が，3 つのエンティティすべてから検証に用いるデータを入手できない．

これらの各ケースにおいて，まず，各方式の検証手続のうちどの処理が実行不可能となるかについて検討する．

4.2 ケース 1：いずれか 1 つのエンティティからデータを入手できない場合

検証者が発行者からデータを入手できない場合，時刻・証拠無方式（NN）では，処理 **c** が実行不可能となるため検証者は T を入手できず，タイムスタンプの意味が失われ，検証処理を実行する意味がなくなる．時刻付・証拠無方式（TN）では，処理 **c**，**d** が実行不可能となるため検証者が発行者から E_{TSI} を入手できず，処理 **e**，**f** も実行不可能となる．この結果，実行可能な処理はたかだか処理 **a**，**b** となる．時刻・証拠付方式（TE）では，E_{TSI} がタイムスタンプに含まれており，検証者が発行者からデータを入手できない場合でも処理 **d**，**e**，**f** は実行可能である．この結果，時刻・証拠付方式では，処理 **c** のみが実行不可能になる．

検証者が証拠補強者からデータを入手できない場合，いずれの方式においても処理 **e** のみが実行不可能と

表 2 3 つのケースにおいて実行できない検証処理
Table 2 Infeasible verification operations in three cases.

タイムスタンプ方式	実行不可能な検証処理						
	ケース 1			ケース 2			ケース 3
	発行者からデータを入手できない場合	証拠補強者からデータを入手できない場合	発行依頼者からデータを入手できない場合	発行者と証拠補強者からデータを入手できない場合	発行者と発行依頼者からデータを入手できない場合	証拠補強者と発行依頼者からデータを入手できない場合	
NN	T を入手できない*	**e**	**f**	T を入手できない*		**e, f**	T を入手できない*
TN	**c, d, e, f**	**e**	**f**	**c, d, e, f**		**e, f**	**c, d, e, f**
TE	**c**	**e**	**f**	**c, e**	**c, f**	**e, f**	**c, e, f**

（注）“*” の「T を入手できない」は，検証者が日時データを入手できず，検証処理を実行する意味が失われることを表す．

なる．

また，検証者が発行依頼者からデータを入手できない場合，いずれの方式においても処理 **f** のみが実行不可能となる．

4.3 ケース 2：いずれか 2 つのエンティティからデータを入手できない場合

検証者が発行者と証拠補強者からデータを入手できない場合，時刻・証拠無方式では，検証者が T を入手できず，タイムスタンプの意味が失われ，検証処理を実行する意味がなくなる．また，時刻付・証拠無方式では，処理 **c**，**d**，**e**，**f** が実行不可能となり，実行可能な処理がたかだか処理 **a**，**b** となる．時刻・証拠付方式では，処理 **c**，**e** が実行不可能となる．

検証者が発行者と発行依頼者からデータを入手できない場合，時刻・証拠無方式では，検証者が T を入手できず，タイムスタンプの意味が失われ，検証処理を実行する意味がなくなる．また，時刻付・証拠無方式では，処理 **c**，**d**，**e**，**f** が実行不可能となり，実行可能な処理はたかだか処理 **a**，**b** のみとなる．時刻・証拠付方式では，処理 **c**，**f** が実行不可能となる．検証者が証拠補強者と発行依頼者からデータを入手できない場合，いずれの方式においても処理 **e**，**f** が実行不可能となる．

4.4 ケース 3：3 つのエンティティすべてからデータを入手できない場合

検証者が 3 つのエンティティすべてからデータを入手できない場合，時刻・証拠無方式では，検証者が発行者から T を入手できず，タイムスタンプの意味が失われ，検証処理を実行する意味がなくなる．時刻付・証拠無方式では，処理 **c**，**d**，**e**，**f** が実行不可能となり，実行可能な検証処理はたかだか処理 **a**，**b** となる．また，時刻・証拠付方式では，処理 **c**，**e**，**f** が実行不可能となる．

以上のケース 1〜3 において実行不可能となる検証処理を整理すると，**表 2** のとおりである．表 2 をもとにして各タイムスタンプ方式において実行可能な検証処理を検討する．検証手続 **abcdef** の時刻付・証拠無方式（TN）を例に説明する．まずケース 1 において検証者が発行者からデータを入手できない場合，処理 **c**，**d**，**e**，**f** が実行不可能となるため，実行可能な検証処理は**a**，**b** となる．また，検証者が証拠補強者や発行依頼者からデータを入手できない場合，それぞれ処理 **e**，**f** が実行不可能となるため，実行可能な検証処理はそれぞれ **a**，**b**，**c**，**d**，**f** と，**a**，**b**，**c**，**d**，**e** となる．またケース 2 において検証者が発行者と証拠補強者からデータを入手できない場合，処理 **c**，**d**，**e**，**f** が実行不可能となるため，実行可能な検証処理は**a**，**b** となる．検証者が発行者と発行依頼者からデータを入手できない場合も同様の結果となり，実行可能な検証処理は**a**，**b** である．検証者が証拠補強者および発行依頼者からデータを入手できない場合，処理 **e**，**f** が実行不可能となるため，実行可能な検証処理は**a**，**b**，**c**，**d** である．最後にケース 3 では，処理 **c**，**d**，**e**，**f** が実行不可能となるため，実行可能な検証処理は**a**，**b** となる．

このような手続きによって，各タイムスタンプ方式と実行可能な検証処理との関係を整理する．まず，表 2 に示された 7 つの場合のうち，検証者が発行者からデータを入手できる 3 つの場合，すなわち，ケース 1 の中で検証者が証拠補強者や発行依頼者からデータを入手できない場合と，ケース 2 の中で検証者が証拠補強者および発行依頼者からデータを入手できない場合について検討する．これらの場合では，タイムスタンプ方式が時刻・証拠付方式，時刻付・証拠無方式，時刻・証拠無方式のいずれにおいても，処理 **e** や処理 **f** が実行不可能になるだけである．これに対し，検証者が発行者からデータを入手できない 4 つの場合，すなわち，検証者が発行者からデータを入手できない場合，発行者と証拠補強者からデータを入手できない場合，発行者と発行依頼者からデータを入手できない場合，3 つのエンティティすべてからデータを入手できない場合においては，タイムスタンプ方式の形態によって各ケースにおける実行可能な検証処理が異なってくる．特に，時刻・証拠無方式の場合，検証者が日

表 3 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
Table 3 Feasible verification operations in cases that the verifier cannot obtain data for the verification from the issuer.

実行可能な検証処理	タイムスタンプ方式			
	ケース 1 の中で発行者からデータを入手できない場合	ケース 2		ケース 3 3 つのエンティティからデータを入手できない場合
		発行者と証拠補強者からデータを入手できない場合	発行者と発行依頼者からデータを入手できない場合	
a	TN-**a**, **ac**, TE-A-**a**, **ac** TN-A-**ad**, **acd**, **ade**, **acde** TN-A-L-**adf**, **acdf**, **adef**, **acdef**	TN-A-**ade**, **acde** TN-A-L-**adef**, **acdef** TE-A-**ae**, **ace**	TN-A-L-**adf**, **acdf**, **adef** **acdef** TE-A-L-**af**, **acf**	TN-A-L-**adef**, **acdef** TE-A-L-**aef**, **acef**
a, **b**	TN-**ab**, **abc** TN-A-**abd**, **abcd**, **abde**, **abcde** TN-A-L-**abdf**, **abcdf**, **abdef**, **abcdef** TE-A-**ab**, **abc**	TN-A-**abde**, **abcde** TN-A-L-**abdef**, **abcdef** TE-A-**abe**, **abce**	TN-A-L-**abdf**, **abcdf**, **abdef**, **abcdef** TE-A-L-**abf**, **abcf**	TN-A-L-**abdef**, **abcdef** TE-A-L-**abef**, **abcef**
a, **d**	TE-A-**ad**, **acd**	TE-A-**ade**, **acde**	TE-A-L-**adf**, **acdf**	TE-A-L-**adef**, **acdef**
a, **e**	TE-A-**ae**, **ace**	該当する方式はなし	TE-A-L-**aef**, **acef**	該当する方式はなし
a, **f**	TE-A-L-**af**, **acf**	TE-A-L-**aef**, **acef**	該当する方式はなし	
a, **b**, **d**	TE-A-**abd**, **abcd**	TE-A-**abde**, **abcde**	TE-A-L-**abdf**, **abcdf**	TE-A-L-**abdef**, **abcdef**
a, **b**, **e**	TE-A−**abe**, **abce**	該当する方式はなし	TE-A-L-**abef**, **abcef**	該当する方式はなし
a, **b**, **f**	TE-A-L-**abf**, **abcf**	TE-A-L-**abef**, **abcef**	該当する方式はなし	
a, **d**, **e**	TE-A-**ade**, **acde**	該当する方式はなし	TE-A-L-**adef**, **acdef**	
a, **d**, **f**	TE-A-L-**adf**, **acdf**	TE-A-L-**adef**, **acdef**	該当する方式はなし	
a, **e**, **f**	TE-A-L-**aef**, **acef**	該当する方式はなし		
a, **b**, **d**, **e**	TE-A-**abde**, **abcde**		TE-A-L-**abdef**, **abcdef**	
a, **b**, **d**, **f**	TE-A-L-**abdf**, **abcdf**	TE-A-L-**abdef**, **abcdef**	該当する方式はなし	
a, **b**, **e**, **f**	TE-A-L-**abef**, **abcef**	該当する方式はなし		
a, **d**, **e**, **f**	TE-A-L-**adef**, **acdef**			
a, **b**, **d**, **e**, **f**	TE-A-L-**abdef**, **abcdef**			

（注）たとえば，TE-A-L-**abdf** は，検証手続 **abdf** を用いる時刻・証拠付—取得型—連鎖型方式を表す．また，たとえば，TN-**ac** は，TN-A-I-**ac**，TN-U-I-**ac**，TN-A-L-**ac**，TN-U-L-**ac** の 4 種類の方式を意味する．

時データ T を入手できず，タイムスタンプとしての意味が失われ検証処理を実行する意味がなくなってしまう．また，時刻・証拠付方式と時刻付・証拠無方式の場合については，**表 3** に整理したとおりである．

4.5 検証手続の可用性によるタイムスタンプ方式の分類

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」という観点から検証手続の可用性を検討している．したがって，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・比較する方法としては，実行可能な検証処理の数に基づいて行う方法と，実行可能な検証処理の種類に基づいて行う方法の 2 つが考えられる．これらのうち，本稿において前提としている検討の枠組みの下で，どちらの方法を採用することが相対的に有用かを考える．

実行可能な検証処理の種類に基づいて分類・比較を行う場合，比較の対象となるタイムスタンプ方式によっては，検証処理の比較を行うことが困難な場合がある．例として，検証者が発行者からデータを入手不可能な場合に，TE-A-I-**abde** と TE-A-L-**abcef** を比較する．各方式における実行可能な検証処理をみると，TE-A-I-**abde** では処理 **a**，**b**，**d**，**e** が実行可能であり，TE-A-L-**abcef** では処理 **a**，**b**，**e**，**f** が実行可能である．これらを比較する場合，3 つの処理 **a**，**b**，**e** は両方の方式に共通しているため，残りの処理 **d** と処理 **f** を比較することが必要となる．しかし，表 2, 3 に示されているように，各検証処理が実行可能か否かはタイムスタンプの種類に依存するため，可用性の観点から検証処理自体を直接比較することは困難である．一方，実行可能な検証処理の数に基づいて分類・比較を行う場合には，検証処理の種類を考慮しないため，実行可能な検証処理の種類が分類・比較に反映されないものの，検証処理間で比較を行う必要がなく，本稿で前提としている検討の枠組みの下で分類・比較を容易に行うことができるという点で有用である．

これらの点をふまえ，本稿において前提としている検討の枠組みの中でタイムスタンプ方式の分類・比較を行うことができるという点に着目し，実行可能な検証処理の数に基づいて分類・比較を行うこととする．

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，実行可能な検証処理数の絶対数をベンチマークとする方法と，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ベンチマークとする方法の 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ベンチマークとすると，タイムスタンプ方式によって既定の検証処理数が様々であるため，本稿で前提としている検討内容と整合的な結果が得られない場合がある．たとえば，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検証手続の可

用性に関して TN-A-I-**abc** と TN-A-I-**abcde** を比較すると，表 3 から，これらの方式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 **b**）の数（ともに 2）の割合はそれぞれ 2/3，2/5 となり，TN-A-I-**abc** の方が望ましいという結果となる．しかし，3.4 節において説明したように，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．このように，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ベンチマークとしたときに，本稿において前提としている検討内容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用いる場合には，既定の検証処理数を考慮しないため，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用いる場合のような不都合が発生しない．また，検証手続の可用性と安全性の両方を考慮してタイムスタンプ方式の評価を行う際に，タイムスタンプの改ざんを検出不可能という意味でタイムスタンプの改ざん攻撃に対して特に注意が必要な方式を容易に見つけることができる．詳細な説明は 5 章に述べるが，文献 18) では，タイムスタンプの改ざん攻撃に対する安全性がその方式の検証手続に依存し，検証手続が **a** である方式では，検証者がタイムスタンプの改ざんを検出不可能であることが示されている．したがって，可用性と安全性の両方を考慮した場合，ケース 1 において実行可能な検証処理数が 1 となる方式では，処理 **a** が必須な処理であることから，ケース 1 における実行可能な検証処理が **a** のみであり，検証者がタイムスタンプの改ざんを検出不可能であることをただちに知ることができる．

こうしたことから，本稿では，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）をベンチマークとしてタイムスタンプ方式の分類・比較を行う．

まず，ケース 1 においては，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ことが考えられる．このような場合には，最も少ない検証処理数をケース 1 の実行可能な検証処理数に対応させることとする．すなわち，実行可能な検証処理に関する最悪のケースに基づいて方式の分類を行う．たとえば，検証手続 **abde** の時刻付・証拠無方式では，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** の 2 つであり，検証者が証拠補強者からデータを入手できない場合には，実行可能な検証処理は処理 **a**，**b**，**d** の 3 つであることから，ケース 1 における実行可能な検証処理数は 2 となる．ケース 2 においても同様の状況が想定されるが，その場合にはケース 1 と同様に最も少ない検証処理数を対応させる．

また，タイムスタンプ方式によってはケース 2 とケース 3 があてはまらない場合もある．たとえば，検証手続 **abde** の時刻付・証拠無方式では，検証者が発行者と証拠補強者からそれぞれデータを入手する反面，発行依頼者からはデータを入手しないため，ケース 3 があてはまらない．このような場合，ケース 2 での実行可能な検証処理数をケース 3 に対応させることとする．たとえば，検証手続 **abde** の時刻付・証拠無方式では，ケース 2 における実行可能な検証処理数が 2 であることから，ケース 3 における実行可能な検証処理数も 2 とする．なお，ケース 2 とケース 3 があてはまらない方式に関しては，ケース 1 の実行可能な検証処理数をケース 2，3 に対応させる．

このようにして各タイムスタンプ方式を対象として実行可能な検証処理数を調べる．たとえば，ケース 1，2，3 における実行可能な検証処理数がそれぞれ 5，4，3 となる方式の集合を (5, 4, 3) と表すこととする．検証者が日時データ T を入手できず，検証処理を実行する意味がなくなる場合には “N”（Nonsense）という記号を用いて表すこととする．

この結果，**表 4** に示すように，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 通りに分類される．これらの分類のうち，時

表 4 検証手続の可用性によるタイムスタンプ方式の分類
Table 4 Classification of time stamping schemes from the availability of the verification procedure.

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**, TE-A-L-**abf, adf** TN-A-**abd, abcd, abde, abcde** TN-A-L-**abf, adf, abdf, abcdf, abdef, abcdef** TE-A-**ab, ad, abc, abe, acd, ade**
(2, 1, 1)	TE-A-**ace**, TE-A-L-**acf, aef**
(1, 1, 1)	TN-**a, ac**, TE-A-**a, ac, ae**, TE-A-L-**af** TN-A-**ad, acd, ade, acde** TN-A-L-**adf, acdf, adef, acdef**
(N, N, N)	NN

（注）たとえば，(5, 4, 3) はケース 1, 2, 3 での実行可能な検証処理数がそれぞれ 5, 4, 3 であることを意味する．

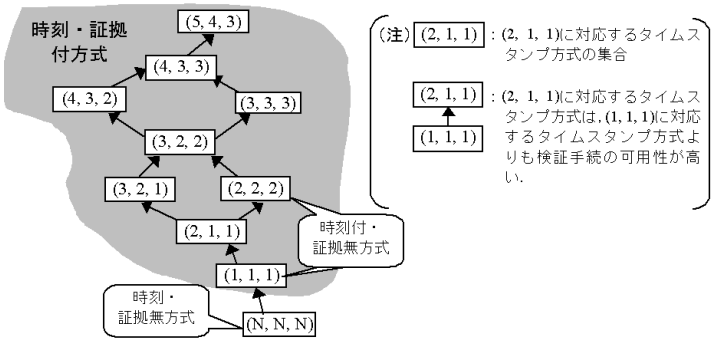

図 2 検証手続の可用性による各タイムスタンプ方式間の関係
Fig. 2 Relationships between time stamping schemes with respect to the availability of the verification procedure.

刻・証拠付方式は (N, N, N) を除く 9 つのカテゴリに分類されるほか，時刻付・証拠無方式は (2, 2, 2) と (1, 1, 1) に，時刻・証拠無方式は (N, N, N) に分類される．このうち，(N, N, N) に対応するタイムスタンプ方式（時刻・証拠無方式のすべて）は，ケース 1〜3 のいずれにおいても検証者が日時データを入手できなくなり，タイムスタンプとしての意味をなさないことが分かる．また，(1, 1, 1) に対応するタイムスタンプ方式（時刻・証拠付方式および時刻付・証拠無方式の一部）は，ケース 1〜3 のいずれにおいても処理 **a** しか実行できなくなる．ここで，処理 **a** は，検証対象となっているデータとタイムスタンプとの対応関係をハッシュ値の比較によって確認するという処理であり，タイムスタンプの一貫性確認や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との間の整合性確認等の高度な検証を実施するものではないことに注意が必要である．

4.6 各タイムスタンプ方式間の関係

次に，表 4 で分類したタイムスタンプ方式の集合間の関係を検討する．たとえば，タイムスタンプ方式の 2 つの集合 X と Y を比較する場合を考える．X と Y の各ケースにおける実行可能な検証処理数を比較し，次のいずれかが該当する場合，「X は Y よりも検証手続の可用性が高い」と表すこととする．

- すべてのケースにおいて，X の実行可能な検証処理数が Y よりも多い．
- 少なくとも 1 つのケースにおいて X の実行可能な検証処理数が Y よりも多く，他のケースでは両者が同じとなる．

このようにしてタイムスタンプ方式の各集合間の関係を検討した結果は**図 2** のとおりである．

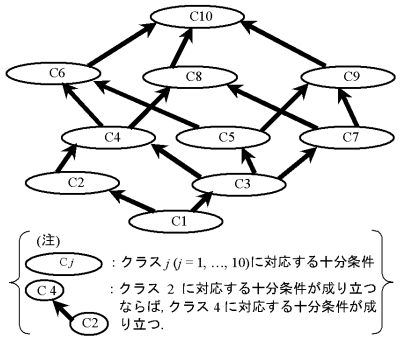

図 3 タイムスタンプの改ざんを検出するための十分条件の関係
Fig. 3 Relationships between conditions sufficient to detect alteration of a time stamp.

5. 可用性と安全性を考慮したタイムスタンプ方式の分類

5.1 文献 18) の研究結果

文献 18) の安全性に関する研究は，検証者がタイムスタンプの改ざんを検出するためにはどのような条件が成立すれば十分かを明らかにするものである．具体的には，各タイムスタンプ方式を対象にタイムスタンプの改ざんを検出するための十分条件（以下，単に十分条件と呼ぶ）を導出し，十分条件には 10 通りのバリエーションがあることを示した．また，各十分条件に対応するタイムスタンプ方式の集合をクラスと定義し，各十分条件間の関係（**図 3** 参照），および，各クラスに属するタイプを明らかにし，タイムスタンプの改ざんに対する安全性が最も高い方式はクラス 10 に対応する方式（検証手続 **abdef**，**abcdef** の時刻・証拠付方式）であることを示した．

なお，文献 18) の検討は，文献 13) における代表的な 2 つの連鎖型方式 Cuculus[4] と PKITS[5] の安全性評価の結果をふまえたうえで行われている．文献 13)

では，Cuculus と PKITS の安全性に関して具体的な仕様に踏み込んだ検討が行われており，文献 18) の検討結果には，そうした連鎖型方式の具体的な仕様に関する考察が反映されている．

5.2 タイムスタンプ方式の分類

文献 18) によって定義されたクラスを用いて，表 4 に分類された各方式がどのクラスに属しているかを整理する．なお，複数のクラスに属するタイムスタンプ方式については，それらのクラスの中で安全性上最も望ましいクラス（以下，基準クラスと呼ぶ）を対応させることとする．各クラスを基準クラスとするタイプを整理すると**表 5** のとおりである．たとえば，(2, 2, 2) に分類される検証処理 **abde** の時刻付・証拠無—取得型—連鎖型方式（TN-A-L-**abde**）は，クラス 1，2，3，4，5，6 に属しており，これらのうち安全性上最も望ましいクラスはクラス 6 であることから，基準クラスはクラス 6 となる．このタイムスタンプ方式のように，安全性の観点で基準クラスがクラス 6 であり，検証手続の可用性の観点で (2, 2, 2) に分類されるタイムスタンプ方式の集合を，以下では (6; 2, 2, 2) と表すこととする．すなわち，第 1 成分が可用性の問題が発生していない場合の基準クラスを表し，第 2〜4 成分がそれぞれケース 1〜3 における実行可能な検証処理数を表す．このような手順でタイムスタンプ方式を分類すると，タイムスタンプ方式は 37 に分類される（**表 6** 参照）．

表 5 基準クラスとタイプ
Table 5 Benchmark classes and their types.

基準クラス	各クラスを基準クラスとするタイプ
1	**a, ae, af, aef**
2	**ab, abe, abf, abef**
3	**ac, ad, acd, ace, acf, acef**
4	**abc, abd, abcd, abce, abcf, abcef**
5	**ade, acde**
6	**abde, abcde**
7	**adf, acdf**
8	**abdf, abcdf**
9	**adef, acdef**
10	**abdef, abcdef**

（注）たとえば “**abcdef**” はタイプ**abcdef** を表す．

次に，これらの集合間の関係を検討する．たとえば，タイムスタンプ方式の 2 つの集合 X と Y を比較する場合を考える．X と Y に対応する基準クラス，および，各ケースにおける実行可能な検証処理数を比較し，次のいずれかが満たされる場合，「X は，安全性および可用性の観点で Y に勝る」と表現する．

- X の基準クラスに対応する十分条件が Y の基準クラスに対応する十分条件よりも弱く，X が Y よりも検証手続の可用性が高い．
- X と Y の基準クラスが同一であり，X が Y よりも検証手続の可用性が高い．
- X の基準クラスに対応する十分条件が Y の基準クラスに対応する十分条件よりも弱く，X と Y が実行可能な検証処理の観点で同じカテゴリに分類される．

このようにして各タイムスタンプ方式の関係を整理した結果は**図 4** のとおりである．図 4 における 2 つのシャドーは，ケース 1〜3 における基準クラスがクラス 1 となるタイムスタンプ方式の集合と，ケース 1

表 6 可用性と安全性を考慮したタイムスタンプ方式の分類
Table 6 Classification of time stamping schemes by the availability and the integrity.

		安全性の観点からの分類（基準クラス）									
		10	9	8	7	6	5	4	3	2	1
検証手続の可用性の観点からの分類	(5, 4, 3)	TE-A-L **-abcdef**	該当する方式なし								
	(4, 3, 3)	TE-A-L **-abdef**	該当する方式なし	TE-A-L **-abcdf**	該当する方式なし	TE-A **-abcde**	該当する方式なし				
	(4, 3, 2)	該当する方式なし	TE-A-L **-acdef**	該当する方式なし				TE-A-L **-abcef**	該当する方式なし		
	(3, 3, 3)	該当する方式なし		TE-A-L **-abdf**	該当する方式なし	TE-A **-abde**	該当する方式なし	TE-A **-abd, abcd**	該当する方式なし		
	(3, 2, 2)	該当する方式なし	TE-A-L **-adef**	該当する方式なし	TE-A-L **-acdf**	該当する方式なし	TE-A **-acde**	TE-A-L-**abcf** TE-A-**abce**	該当する方式なし	TE-A-L **-abef**	該当する方式なし
	(3, 2, 1)	該当する方式なし							TE-A-L-**acef**	該当する方式なし	
	(2, 2, 2)	TN-A-L **-abdef, abcdef**	該当する方式なし	TN-A-L **-abdf, abcdf**	TE-A-L **-adf**	TN-A **-abde abcde**	TE-A **-ade**	TN-**abc** TN-A **-abd, abcd** TE-A-**abc**	TE-A **-ad, acd**	TN-**ab** TE-A-L-**abf** TE-A **-ab, abe**	該当する方式なし
	(2, 1, 1)	該当する方式なし							TE-A-L-**acf** TE-A-**ace**	該当する方式なし	TE-A-L-**aef**
	(1, 1, 1)	該当する方式なし	TN-A-L **-adef, acdef**	該当する方式なし	TN-A-L **-adf, acdf**	該当する方式なし	TN-A **-ade, acde**	該当する方式なし	TN-**ac** TN-A-**ad, acd** TE-A-**ac**	該当する方式なし	TN-**a** TE-A-L-**af** TE-A-**a, ae**
	(N, N, N)	NN-A-L **-abcdef**	NN-A-L **-acdef**	NN-A-L **-abdf, -abcdf**	該当する方式なし	NN-A **-abcde**	NN-A **-acde**	NN-U-**abc** NN-A **-abc, abcd**	NN-U-**ac** NN-A-**ac, acd**	該当する方式なし	

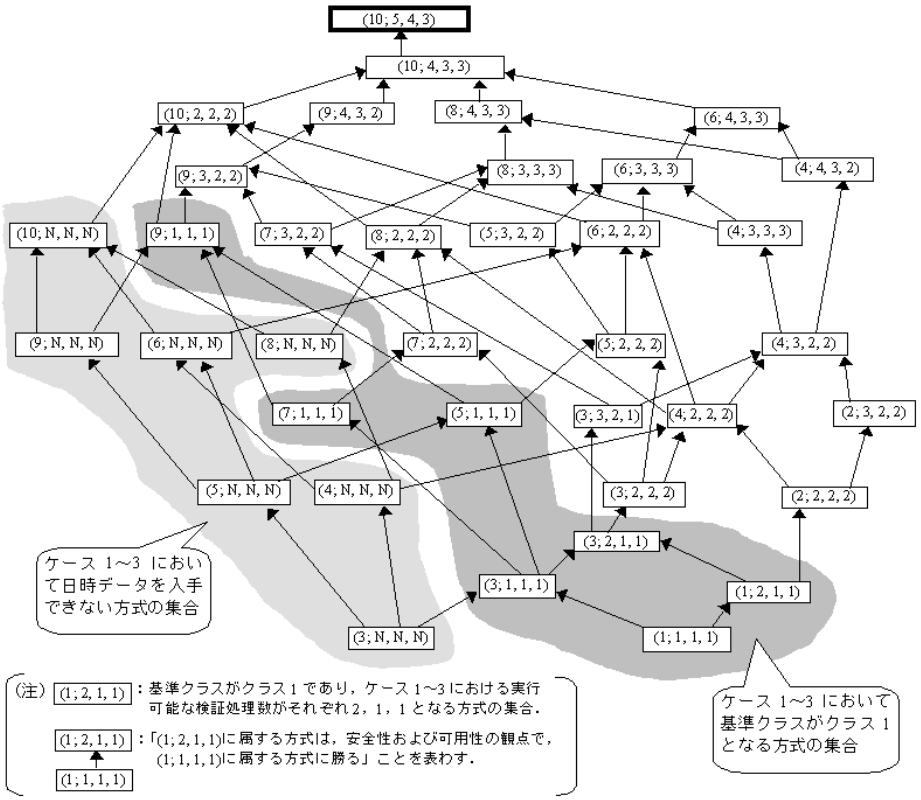

図 4 可用性と安全性による各タイムスタンプ方式間の関係
Fig. 4 Relationships between time stamping schemes from the viewpoints of the availability and the integrity.

〜3 において検証者が日時データを入手できないタイムスタンプ方式の集合をそれぞれ示している．ケース 1〜3 において基準クラスがクラス 1 となる方式の集合は，(9; 1, 1, 1)，(7; 1, 1, 1)，(5; 1, 1, 1)，(3; 1, 1, 1)，(1; 1, 1, 1)，(3; 2, 1, 1)，(1; 2, 1, 1) であり，検証者が日時データを入手できない方式の集合は，(10; N, N, N)，(9; N, N, N)，(8; N, N, N)，(6; N, N, N)，(5; N, N, N)，(4; N, N, N)，(3; N, N, N) である．すでに 4.5 節において検証手続の可用性の観点からこれらの方式を利用する際の留意点について説明したが，安全性の観点を加えてタイムスタンプ方式を分類したことによって，たとえば (10; N, N, N) や (9; 1, 1, 1) のように，可用性の問題が発生していないときの基準クラスが比較的上位に位置するタイムスタンプ方式であっても，発行者等からデータを入手できない状況となった場合には，日時データを入手できないとか，処理 **a** しか実行できず基準クラスが実質的にクラス 1 になってしまうといった問題が生じることが判明した．基準クラスがクラス 1 となるタイムスタンプ方式では，検証者がタイムスタンプの改ざんを検出不可能であることが示されている[18]．こうした観点からみると，実行可能な検証処理数による分類において (N, N, N) や (1, 1, 1) に分類されるタイムスタンプ方式の利用には注意が必要であると考えられる．

また，あるタイムスタンプ方式のセキュリティ評価を行う際に，表 6 や図 4 の結果を用いることによって，その方式の詳細な仕様に立ち入ることなく可用性および安全性上の特性を比較的容易に把握することができる．すなわち，タイムスタンプに含まれるデータ，検証者における E_{TSI} の取得可能性，タイムスタンプの生成方法，タイムスタンプの検証手続という 4 点に着目し，評価対象のタイムスタンプ方式がどのグループ，タイプに属するかを検討し，表 6 のどのカテゴリに分類されるかを調べることによって，その方式における実行可能な検証処理数や，安全性評価を行う際にどのような点を確認する必要があるか（たとえば，発行者や証拠補強者が攻撃者と結託する可能性）が分かる．

さらに，検証者が特定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，タイムスタンプの改ざんに対する安全性がどのように変化するかを容易

表 7 7 つのタイムスタンプ方式の特徴
Table 7 Characteristics of seven existing time stamping schemes.

タイムスタンプ方式	主なタイムスタンプ構成データ	エンティティ	タイムスタンプ検証手続	分類		
				グループ	タイプ	安全性と可用性による分類
電子公証制度 時刻署名分散システム	H, ID_{TSI}, T, ID_{REQ}, $Info_{INT}$	発行者, 発行依頼者	(1) ハッシュ値を比較（処理 **a**） (2) ディジタル署名を検証（処理 **b**）	TN-U-I	**ab**	(2; 2, 2, 2) クラス $2^{(1)}$ **a**, **b**$^{(2)}$
Digital Notary /SecureSeal	H, ID_{TSI}, T, ID_{REQ}	発行者, 発行依頼者, 証拠補強者（新聞）	(1) ハッシュ値を比較（処理 **a**） (2) 発行者にタイムスタンプを送り，検証を依頼（処理 **c**）	TN-U-L	**ac**	(3; 1, 1, 1) クラス $1^{(1)}$ **a**$^{(2)}$
Benaloh と de Mare のプロトコル	H, ID_{TSI}, T, E_{TSI}	発行者, 発行依頼者	(1) ハッシュ値を比較（処理 **a**） (2) タイムスタンプを構成するデータ（E_{TSI} に対応）とハッシュ関数を用いて一定の演算を実行（処理 **d**）	TE-A-L	**ad**	(3; 2, 2, 2) クラス $3^{(1)}$ **a**, **d**$^{(2)}$
PKITS	H, ID_{TSI}, T, ID_{REQ}, $Info_{INT}$, ID_{AMP}	発行者, 発行依頼者, 証拠補強者（他の発行者）	(1) ハッシュ値を比較（処理 **a**） (2) ディジタル署名を検証（処理 **b**） (3) 発行者から得たデータ（E_{TSI} に対応）から連鎖データを再生し，その整合性を確認（処理 **d**） (4) 他の発行者から入手した連鎖データと再生した連鎖データを比較（処理 **e**）	TN-A-L	**abde**	(6; 2, 2, 2) クラス $2^{(1)}$ **a**, **b**$^{(2)}$
TIMESEC		発行者, 発行依頼者, 証拠補強者（インターネット上のサイト）	(1) ハッシュ値を比較（処理 **a**） (2) ディジタル署名を検証（処理 **b**） (3) 発行者から得たデータ（E_{TSI} に対応）から連鎖データを再生し，その整合性を確認（処理 **d**） (4) インターネット上のサイトから入手した連鎖データを比較（処理 **e**）			
Cuculus	H, ID_{TSI}, T, ID_{REQ}, $Info_{INT}$, ID_{AMP}, E_{TSI}	発行者, 発行依頼者, 証拠補強者（新聞）	(1) ハッシュ値を比較（処理 **a**） (2) ディジタル署名を検証（処理 **b**） (3) タイムスタンプを構成するデータ（E_{TSI} に対応）から連鎖データを再生し，その整合性を確認（処理 **d**） (4) 連鎖データと新聞掲載の連鎖データを比較（処理 **e**）	TE-A-L	**abde**	(6; 3, 3, 3) クラス $4^{(1)}$ **a**, **b**, **d**$^{(2)}$

（注）「安全性と可用性による分類」の欄の (1) と (2) は，ケース 1〜3 の場合の基準クラス，実行可能な検証処理をそれぞれ表す．

に検討することができる．たとえば，検証処理 **abde** の時刻付・証拠無方式の場合，検証者が既定の検証処理を実行できる場合には基準クラスがクラス 6 となるものの，検証者が発行者から検証に用いるデータを入手できなくなると，実行可能な検証処理は処理 **a**，**b** の 2 つとなり，検証手続 **ab** のタイムスタンプ方式の基準クラスであるクラス 2 となってしまう．これは，検証者が発行者からデータを入手できなくなると，タイムスタンプの改ざん攻撃に対する安全性が低下することを意味している．このように，サービス提供者が廃業した場合，あるいは，サービス妨害攻撃等を受けて機能を停止した場合等に，タイムスタンプ方式の安全性が低下する可能性がある点にも留意しておく必要がある．

6. 主要なタイムスタンプ方式への適用

本稿における検討結果を既存のタイムスタンプ方式に適用する．ここでは，タイムスタンプ発行・検証手続等が公開されている主な方式として，法務省・電子公証制度[6]，時刻署名分散システム[12]，Cuculus[3),4)]，PKITS[5]，TIMESEC[10]，Digital Notary[11]/SecureSeal[9]，Benaloh と de Mare のプロトコル[2] を取り上げる（**表 7** 参照）．

まず，電子公証制度と時刻署名分散システムは，検証手続 **ab** を用いる時刻付・証拠無—非取得型—個別型方式（TN-U-I-**ab**）に分類され，既定の検証手続における基準クラスがクラス 2 に対応することから (2; 2, 2, 2) に分類される．これらの方式では，検証者が発行者からデータを入手することなく検証を実行するため，検証者はケース 1〜3 のいずれにおいても既定の検証処理 **a**，**b** を実行可能であることが分かる．また，安全性に関しては，ケース 1〜3 のいずれにおいても基準クラスはクラス 2 となることが分かる．

Digital Notary/SecureSeal は，検証手続 **ac** の時刻付・証拠無—非取得型—連鎖型方式（TN-U-L-**ac**）に分類され，既定の検証手続における基準クラスがクラス 3 となることから (3; 1, 1, 1) に分類される．ケース 1〜3 のいずれの場合においても実行可能な検証処理は処理 **a** のみとなり，実行できる検証処理が減少することが分かる．また，安全性の観点では，ケース 1〜3 のいずれの場合でも基準クラスがクラス 3 からクラス 1 に変化することが分かる．このため，Digital Notary/SecureSeal に類似のタイムスタンプ方式を利用する場合，検証者が発行者からデータを確実に入手

するための対策が十分に講じられているかを確認しておく必要があると考えられる．

Benaloh と de Mare のプロトコルは，検証手続 **ad** の時刻・証拠付—連鎖型方式（TE-A-L-**ad**）に分類され，既定の検証手続における基準クラスがクラス 3 となることから (3; 2, 2, 2) に分類される．Benaloh と de Mare のプロトコルでは，タイムスタンプに E_{TSI} が含まれ，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も既定の検証処理 **a**，**d** ともに実行可能であることが分かる．また，安全性の観点では，ケース 1〜3 のいずれにおいても基準クラスがクラス 3 となることが分かる．

PKITS と TIMESEC は，検証手続 **abde** の時刻付・証拠無—取得型—連鎖型方式（TN-A-L-**abde**）に分類され，既定の検証手続における基準クラスがクラス 6 となることから (6; 2, 2, 2) に分類される．これらの方式では，ケース 1〜3 のいずれの場合においても実行可能な検証処理が処理 **a**，**b** の 2 つとなり，実行できる検証処理が減少することが分かる．また，安全性の観点では，ケース 1〜3 のいずれの場合も基準クラスはクラス 6 からクラス 2 に変化し，タイムスタンプの改ざん攻撃に対する安全性が低下することが分かる．

Cuculus は，検証手続 **abde** の時刻・証拠付—連鎖型方式（TE-A-L-**abde**）に分類され，既定の検証手続における基準クラスがクラス 6 となることから (6; 3, 3, 3) に分類される．Cuculus では，ケース 1〜3 のいずれの場合においても実行可能な検証処理は処理 **a**，**b**，**d** の 3 つとなり，実行可能な検証処理が減少することが分かる．また，安全性の観点では，ケース 1〜3 のいずれにおいても基準クラスはクラス 6 からクラス 4 に変化し，タイムスタンプの改ざん攻撃に対する安全性が低下することが分かる．

検証者が各エンティティからデータを入手できない場合を前提として，上記 7 つのタイムスタンプ方式の安全性を比較すると，まず Cuculus は，ケース 1〜3 のいずれにおいても基準クラスがクラス 4 となり，他の 6 つの方式よりも安全性上望ましいことが分かる．また，ケース 1〜3 において，PKITS，TIMESEC，電子公証制度，時刻署名分散システムは基準クラスがクラス 2 となるほか，Benaloh と de Mare のプロトコルは基準クラスがクラス 3，Digital Notary/SecureSeal は基準クラスがクラス 1 となる．したがって，PKITS，TIMESEC，電子公証制度，時刻署名分散システム，Benaloh と de Mare のプロトコルは，Digital Notary/SecureSeal よりもケース 1〜3 において安全性上望ましいことが分かる．

7. おわりに

本稿では，タイムスタンプ方式に対する可用性，特に検証者が各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に焦点を絞り，各タイムスタンプ方式の特徴や，各方式間の関係について検討した．まず，タイムスタンプ方式に対する可用性を定義し，どのような場合に可用性が損なわれるかを整理した．そのうえで，各方式に関して，検証者が各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どの検証処理が実行可能かを示した．さらに，文献 18) の安全性に関する検討結果を用いて可用性と安全性の両面からタイムスタンプ方式を 37 に分類し，各方式間の関係を明らかにした．文献 18) の検討結果には，文献 13) における連鎖型方式の具体的な仕様に関する考察が反映されており，本稿での安全性に関する検討結果も，連鎖型方式の具体的な仕様をふまえたものとなっている．最後に，7 つの主要なタイムスタンプ方式に本検討結果を適用し，本稿における検討結果を活用することによって，タイムスタンプ方式の詳細な仕様に立ち入ることなく，可用性および安全性上の特性を比較的容易に把握することが可能になることを示した．

今後の課題として，まず，タイムスタンプ方式に対する可用性を損なう問題が発生する可能性について検討を行い，その結果を用いて可用性に関する検討を深めることがあげられる．今回の検討では，可用性が損われることを前提としており，そうした問題が発生する可能性がどの程度について考慮していなかった．また，安全性と可用性だけでなく，タイムスタンプを実装する際にかかるコストについても考慮して各タイムスタンプ方式の評価を行うことが第 2 の課題としてあげられる．

謝辞 本研究は，一部分，文部科学省科学研究費補助金特定領域研究 13224040（松本 勉）の支援を受けて行われた．

参考文献

1) Adams, C., Cain, P., Pinkas, D. and Zuccherato, R.: RFC 3161: Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP) (2001). http://www.ietf.org/rfc/rfc3161.txt
2) Benaloh, J. and de Mare, M.: One-Way Accumulators: A Decentralized Alternative to Digital Signature, *Proc. EUROCRYPT'93*, LNCS

765, pp.274–285, Springer-Verlag (1994).
3) Buldas, A., Lipmaa, H. and Schoenmakers, B.: Optimally Efficient Accountable Time-Stamping, *Proc.PKC2000*, LNCS 1751, pp.293–305, Springer-Verlag (2000).
4) Cybernetica: Cuculus: How does it work? (2001). http://www.cyber.ee/research/cuc-work. html, the access date: October 9, 2001.
5) Fabrica Nacional de Moneda y Timbre: PKITS: Deliverable D4a Description and Results of the Unstructured Data Time-Stamping Protocol Implementation, Revision Number 16 (1998). http://www.fnmt.es/pkits/
6) 法務省民事局：電子取引法制に関する研究会報告書 (1998).
7) International Organization for Standardization and International Electrotechnical Commission: ISO/IEC TR 13335: Information technology—Security techniques—Guidelines for the Management of IT Security (1997).
8) International Organization for Standardization and International Electrotechnical Commission: ISO/IEC WD 18014-1: Information technology—Security techniques—Time stamping service—Part 1: General (2001). http://csrc.nist.gov/cc/t4/sc27/post-london-files/27n2595.pdf, the access date: October 9, 2001.
9) NTT データ：SecureSeal 〈テクニカル情報〉 (2001). http://210.144.76.11/technical /tech01. html, the access date: October 9, 2001.
10) Preneel, B., Rompay, B.V., Quisquater, J.J., Massias, H. and Avila, J.S.: Design of a Timestamping System, TIMESEC Technical Report WP3 (1998). http://www.dice.ucl.ac.be/crypto /TIME SEC/TR3.ps.gz
11) Surety.com: Secure Time/Data Stamping in a Public Key Infrastructure (2001). http://www.surety.com/home/pki.pdf, the access date: October 9, 2001.
12) Takura, A., Ono, S. and Naito, S.: Secure and Trusted Time Stamping Authority, *Proc. IWS'99*, pp.123–128, Springer-Verlag (1999).
13) 宇根正志，松本　勉：タイムスタンププロトコル Cuculus と PKITS の安全性に関する一考察，情報処理学会研究報告，2000-CSEC-11，pp.55–60 (2000).
14) 宇根正志，松本　勉：連鎖型タイムスタンプの検証に用いられる情報の管理，コンピュータセキュリティシンポジウム 2000 予稿集，pp.25–30 (2000).
15) 宇根正志，松本　勉：タイムスタンプの安全性と検証手続との関連性，2001 年暗号と情報セキュリティ・シンポジウム予稿集，pp.629–634, 電子情報通信学会 (2001).
16) 宇根正志，松本　勉：タイムスタンプ方式における 10 の安全性クラス，情報処理学会研究報告，2001-CSEC-14, pp.141–148 (2001).
17) 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 (2001).
18) Une, M. and Matsumoto, T.: 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 (2002).

(平成 13 年 11 月 30 日受付)
(平成 14 年 6 月 4 日採録)

宇根　正志（学生会員）

昭和 46 年生．平成 6 年筑波大学第三学群社会工学類卒業．同年日本銀行入行．平成 8 年より日本銀行金融研究所に所属し，金融分野に関連の深い情報セキュリティ技術の研究に従事．平成 12 年からは，横浜国立大学大学院工学研究科博士課程後期に在籍．電子情報通信学会学生会員．

松本　勉（正会員）

昭和 33 年生．昭和 61 年東京大学大学院博士課程（電子工学）修了，工学博士．同年横浜国立大学工学部専任講師．現在，同大学大学院環境情報研究院教授．昭和 56 年より主として暗号や情報セキュリティの研究・教育に従事．「明るい暗号研究会」を数人の仲間とともに創り研究を始めた．国際暗号学会 IACR 理事．ASIACRYPT '96 プログラム委員長．ASIACRYPT 2000（国際暗号学会主催）実行委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．