マルチメディア通信と分散処理　101－6
コンピュータセキュリティ　12－6
（２００１．２．２０）

時刻・証拠付タイムスタンプの安全性と検証情報管理コスト

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 人工環境システム学専攻
*日本銀行 金融研究所

あらまし
本稿では，まず，タイムスタンプの生成・検証手続に基づく，時刻・証拠付タイムスタンプの分類方法を示す．その上で，宇根・松本[8]の研究成果に基づき，各タイムスタンプの改ざんに対する安全性について検討を行うほか，タイムスタンプの検証に用いられる情報の管理コストについて検討する．本稿では，この管理コストを検証情報管理コストと呼び，タイムスタンプの検証に用いられる情報を通信・保管するコストと，検証手続の処理にかかるコストから構成されるものとする．

Time Stamps with both Time Information and Evidence: Security and Evidence Management Cost

Masashi Une†*　　Tsutomu Matsumoto†
une@mlab.jks.ynu.ac.jp　tsutomu@mlab.jks.ynu.ac.jp
† Division of Artificial Environment and Systems, Graduate School of Engineering
Yokohama National University
*Institute for Monetary and Economic Studies, Bank of Japan

Abstract
In this paper, we first describe a way to classify time stamps with both time information and evidence according to how to generate and verify time stamps. Then, we consider security against alteration of time stamps and cost of managing evidence that is data used to verify time stamps in each class by using a result of Une and Matsumoto[8]. We call the cost "evidence management cost," which consists of communication and storage cost of evidence and cost of carrying out verification procedures.

1　はじめに

タイムスタンプ技術は特定データが特定日時・時刻に存在していたことを証明する技術である．近年電子商取引や電子文書管理を進める動きが活発化する中，タイムスタンプ技術は，電子文書やその取扱履歴を長期間保管するための技術として注目されている．既にタイムスタンプの各種プロトコル[1, 2, 3, 5]が提案されているほか，SecureSeal[4]/Digital Notary[6]等の商用サービスも開始されている．

こうした中，タイムスタンプ方式の安全性確保が重要な課題となっており，安全性評価手法の確立が求められている．宇根・松本[7]は，タイムスタンプの発行・検証手続の枠組みや，タイムスタンプ方式の分類方法を提案した．また，宇根・松本[8]は，タイムスタンプの検証手続に関する概念整理を行い，各検証手続とタイムスタンプの改ざんに対する安全性との関連性について検討した．これらの研究は，タイムスタンプ方式の安全性評価の土台となる概念整理の精緻化を進めるものであるが，時刻・証拠付タイムスタンプ方式に関する検討はこれまでに行われていない．

本稿では，時刻・証拠付タイムスタンプ方式を対象として，宇根・松本[8]の成果を基にタイムスタンプの改ざんに対する安全性について検討するほか，タイムスタンプの検証手続に関連するコストとして検証情報管理コストを定義し，各方式においてどのような検証情報管理コストが必要となるかについて検討する．

まず，2において，時刻・証拠付タイムスタンプ方式の枠組みを説明し，分類を行う．その上で，3では各方式の安全性に関する検討を行い，4では，検証情報管理コストを定義し，11 種類の検証手続を用いる各方式の検証情報管理コストについて検討する．5では，検討結果をまとめ，今後の課題を示す．

2　時刻・証拠付タイムスタンプ方式

2.1　定義

まず，時刻・証拠付タイムスタンプを，「特定データが特定時刻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, ID_{TSI}, T, E_{TSI}, $Info_{INT}$ から構成されるデータ」と定義する[8]．タイムスタンプを構成する各データは以下の通り．

・H：タイムスタンプ対象データ M のハッシュ値．
・ID_{TSI}：タイムスタンプを発行するエンティティ（以下，発行者<time stamp issuer>）の識別データ．

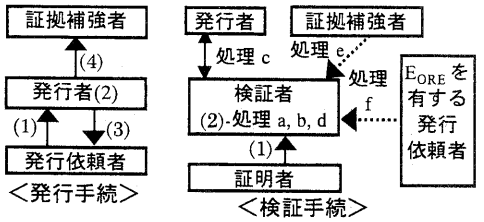

図 1 タイムスタンプの発行・検証手続

・T：タイムスタンプの発行を依頼するエンティティ（以下，発行依頼者<time stamp requester>）から発行者が H を受信する日時・時刻データ．

・E_{TSI}：タイムスタンプを構成するデータが，発行者のデータベース（以下，DB）のデータと整合的であることを確認するデータ（検証情報の 1 つであり，“TSI”は“発行者<time stamp issuer>”を表す）．タイムスタンプはその生成方法によって連鎖型と個別型に分類されるが，連鎖型では，各タイムスタンプを生成する際に，DB に記録されている他のタイムスタンプを読み出し，そのタイムスタンプを構成するデータの一部 E_{ORE}（検証情報の 1 つであり，“ORE”は“他の発行依頼者<other requestors>”を表す）を用いる．このため，タイムスタンプを構成するデータと DB の整合性確認の際に，E_{ORE} を用いることが必要となり，E_{ORE} は E_{TSI} の一部となる．一方，個別型では，タイムスタンプ生成時に他のタイムスタンプを構成するデータを用いない．

・$Info_{INT}$：タイムスタンプを構成するデータの一貫性を確認するデータ．ディジタル署名等が想定される．

2.2 エンティティ

・**発行者**：タイムスタンプを発行．タイムスタンプや，その発行時に生成されるすべてのデータを保管し，検証時に利用する．E_{TSI} の一貫性を確認するデータ E_{AMP}（検証情報の 1 つであり，“AMP”は“証拠補強者<evidence amplifier>”を表す）を生成し，証拠補強者に送る場合もある．

・**発行依頼者**：あるデータ M に対するハッシュ値 H を発行者に送り，M に対するタイムスタンプを入手．連鎖型の方式では，各タイムスタンプの一部が E_{ORE} となり，E_{TSI} の一貫性を確認するデータとして E_{ORE} を検証者に送る場合もある．

・**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付．一般に，証明者は発行依頼者と同一となる．

・**検証者**（verifier）：タイムスタンプ等を用いて，あるデータ M が，T の時点に存在したことを確認．

・**証拠補強者**：E_{AMP} を発行者から入手し，タイムスタンプの検証時に検証者に提供．発行者とは別のエンティティである．例えば，タイムスタンプの検証に使われるデータを新聞に掲載する方式では，新聞と掲載データがそれぞれ証拠補強者と E_{AMP} に対応する．

2.3 タイムスタンプ発行手続（図 1 左参照）

(1)発行依頼者は，タイムスタンプの発行を要求するデータ（H 等を含む）を発行者に送付．

表 1 検証手続によるタイムスタンプの分類

	適用可能な検証手続（処理の組合せ）	
連鎖型の時刻・証拠付タイムスタンプ	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 （合計 32 通り）	処理 a, b, c, d, e, f が適用可能．処理 a は必須．
個別型の時刻・証拠付タイムスタンプ	a, ab, ac, ad, ae, abc, abd, abe, acd, ace, ade, abcd, abce, abde, acde, abcde （合計 16 通り）	処理 a, b, c, d, e が適用可能．処理 a は必須．

（各処理の内容）

・処理 a：検証者が M のハッシュ値と H を比較．

・処理 b：検証者が $Info_{INT}$ によってタイムスタンプを構成するデータの一貫性を確認．

・処理 c：発行者が，検証者から受取ったタイムスタンプと DB に保管されているタイムスタンプを比較．その結果を検証者に通知．

・処理 d：検証者が E_{TSI} によってタイムスタンプを構成するデータと DB のデータとの整合性を確認．

・処理 e：検証者が E_{AMP} によって E_{TSI} の一貫性を確認．

・処理 f：検証者が E_{ORE} によって E_{TSI} の一貫性を確認．

(2)発行者は，タイムスタンプを生成．検証時に証拠補強者や他の発行依頼者が利用される場合，それらの識別データもタイムスタンプに含まれる．

(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，既存のタイムスタンプを構成するデータから E_{AMP} を生成し，証拠補強者に送る場合もある．

2.4 タイムスタンプ検証手続（図 1 右参照）

(1)証明者は検証者に M，H，タイムスタンプ等を送付．

(2)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．

検証手続については，宇根・松本[8]が，検証手続を構成する 6 種類の処理 a～f を定義し，32 通りの検証手続が想定されることを示している．このうち，タイムスタンプに適用可能な検証手続は，連鎖型と個別型で異なり，それぞれ 32，16 の検証手続が対応する（表 1 参照）．連鎖型と個別型で適用可能な検証手続の数が異なるのは，連鎖型では E_{ORE} を用いる処理 f が適用可能な反面，個別型では処理 f が適用不可能なためである．

なお，表 1 の「適用可能な検証手続」に記載されている記号は検証手続の種類を示す．例えば検証 ade は，連鎖型と個別型の両方に適用可能であり，3 つの処理 a, d, e を行う検証手続を意味する．

2.5 時刻・証拠付タイムスタンプ方式の分類

本稿では，時刻・証拠付タイムスタンプ方式を，生成方法によって連鎖型と個別型に分類した上で，連鎖型と個別型の方式を適用可能な検証手続によってそれぞれ 32 通り，16 通りに分類する（表 1 参照）．この結果，時刻・証拠付タイムスタンプ方式は，全体で 48 通りに分類されることとなる．なお，代表的な時刻・証拠付タイムスタンプ方式である Cuculus[2]は，検証手続

表 2 各検証手続におけるタイムスタンプの改ざん検出の難易

検証手続のグループ	攻撃の条件																							
	$Info_{INT}$ の偽造を検出困難												$Info_{INT}$ の偽造を検出容易											
	発行者と結託可能				発行者と結託不可能，なりすまし可能				発行者と結託・なりすまし不可能				発行者と結託可能				発行者と結託不可能，なりすまし可能				発行者と結託・なりすまし不可能			
	w		x		w		x		w		x		w		x		w		x		w		w	
	y	z	y	z	y	z	y	z	y	z	y	z	y	z	y	z	y	z	y	z	y	z	y	z
1	×												×				×							
2	×												×				○							
3	×								○				×								○			
4	×								○				×				○							
5	×		○		×		○						×		○		×				○			
6	×		○		×		○						×				○							
7*	×	○	×	○	×	○	×		○				×	○	×	○	×	○	×		○			
8*	×	○	×	○	×	○	×		○				×	○	×		○							
9*	×		○		×		○						×		○		×		○					
10*	×		○		×		○						×				○							

（検証手続）グループ 1：a, ae, af, aef　　グループ 2：ab, abe, abf, abef　　グループ 3：ac, ad, acd, ace, acf, acef
グループ 4：abc, abd, abcd, abce, abcf, abcef　　グループ 5：ade, acde　　グループ 6：abde, abcde
グループ 7：adf, acdf　　グループ 8：abdf, abcdf　　グループ 9：adef, acdef
グループ 10：abdef, abcdef　　（*が付いているグループ 7～10 の検証手続は連鎖型のみ適用可能）

（凡例）×：タイムスタンプの改ざん検出が困難．　○：タイムスタンプの改ざん検出が容易．（シャドーの部分）
w：攻撃者は，証拠補強者と結託可能，または，証拠補強者になりすまし可能．
x：攻撃者は，証拠補強者と結託不可能，かつ，証拠補強者になりすまし不可能．
y：攻撃者は，E_{ORE} を有する発行依頼者と結託可能，または，E_{ORE} を有する発行依頼者になりすまし可能．
z：攻撃者は，E_{ORE} を有する発行依頼者と結託不可能，かつ，E_{ORE} を有する発行依頼者になりすまし不可能．

として abde を用いる連鎖型の方式に該当する．

3 タイムスタンプの安全性に関する検討

宇根・松本[8]は，32 通りの各検証手続を用いる方式で，タイムスタンプの改ざん検出が困難あるいは容易となる条件を明らかにしている．本節では，その結果を用いてタイムスタンプの安全性について検討する．

3.1 攻撃者と攻撃の目的

攻撃者は発行依頼者の 1 人とする．攻撃の目的は，検証者が検出困難なように，既存のタイムスタンプを構成するデータを改ざんすることとする．

3.2 攻撃の前提

タイムスタンプの生成に利用されるハッシュ関数は second-preimage 探索が計算量的に困難であるとする．つまり，あるタイムスタンプに対応する異なる複数のデータ M の探索が困難であるとする．

また，処理 c，d，e，f において，各処理を行うエンティティが既定の手順に沿ってその処理を正しく実行する場合，各処理に利用されるデータ（処理 e では E_{AMP}）をある 1 つの値に固定したときに，検証が成功する検証対象データ（例えば処理 e では E_{TSI}）を複数個探索することは計算量的に困難であるとする．この前提によって，例えば，検証者が既定の手順に沿って処理 e を正しく実行する状況下では，攻撃者が E_{TSI} を E'_{TSI} に改ざんしたとしても，E_{AMP}（E_{TSI} に対応）の代わりに E'_{AMP}（E'_{TSI} に対応）を検証者に入手させることが不可能ならば，検証者は E_{AMP} を用いて処理 e を実行することによって E'_{TSI} の改ざんを容易に検出できる．

検証者は，各検証の処理において，既定の手順に沿って常に正しく各処理を実行するものとする．

タイムスタンプ発行・検証時の各エンティティ間の通信データは，通信当事者以外に対して守秘性と一貫性が確保されるものとする．

3.3 攻撃の条件

$Info_{INT}$ の偽造を後で検出容易な場合と検出困難な場合に分けて検討するほか，攻撃者が他のエンティティと結託可能な場合と結託不可能な場合に分けて検討する．また，攻撃者が他のエンティティになりすまし可能な場合と不可能な場合に分けて検討する．

3.4 検討結果

上記設定の下で，各方式においてタイムスタンプの改ざん検出の難易に関する条件を検討し，同じ条件になるものを表 2（[8]の表 3 と表 4 を整理したもの）に整理した．表 2 の第 1 列「検証手続のグループ」に，改ざん検出の難易の条件が同じとなる検証手続のグループ（1～10）が示され，第 2 列「攻撃の条件」にその条件が記載されている．記号「○」「×」は，該当する条件下でタイムスタンプの改ざん検出がそれぞれ容易，困難であることを示す．例えば，表 2 のグループ 2 は検証 ab，abe，abf，abef を含み，これらの検証手続を用いた方式においてタイムスタンプの改ざん検出が容易となるのは，$Info_{INT}$ の偽造検出が容易，かつ，攻撃者が発行者と結託不可能な場合であることを示している．

連鎖型の時刻・証拠付タイムスタンプ方式の中でタイムスタンプの改ざんに対する安全性上最も望ましいのは，グループ 10 の検証手続を用いる方式となる．こ

れらの方式では，$Info_{INT}$ の偽造検出が困難な場合も，攻撃者が発行者，証拠補強者，もしくは，E_{ORE} をもつ発行依頼者と結託不可能，かつ，各エンティティになりすまし不可能である限り，改ざんを容易に検出できる．

一方，個別型の時刻・証拠付タイムスタンプ方式で，タイムスタンプの改ざんに対する安全性上最も望ましいものは，グループ 6 の検証手続を用いる方式となる．これらの方式では，$Info_{INT}$ の偽造検出が困難な場合も，攻撃者が発行者や証拠補強者と結託不可能，かつ，これらのエンティティになりすまし不可能である限り，改ざんを容易に検出できる．

連鎖型の方式は，処理 f を含むグループ 7〜10 の検証手続を用いることによって，個別型の方式よりも高い安全性を達成可能である．ただし，グループ 1〜6 の検証手続を用いる方式の安全性を確保すれば十分な場合，連鎖型，個別型どちらでも対応可能である．

なお，グループ 1 の検証手続は，いかなる条件の下でもタイムスタンプの改ざん検出は困難となるため，実際には利用困難と考えられる．

4 検証情報管理コストに関する検討

本節では，各方式を実装する際に必要となる各種コストの中で，検証手続に関連するコストに焦点を当てて検討する．まず検討対象とする検証情報管理コストを定義し，連鎖型の方式間，および，個別型の方式間において検証情報管理コストの比較を行う．

4.1 検証情報管理コスト

検証手続に関連する主なコストとして，3 種類の検証情報 E_{TSI}，E_{AMP}，E_{ORE} の通信・保管コスト，これらを用いた各種検証の処理に伴うコスト，の 3 つが挙げられる．本稿では，これらを合計したものを検証情報管理コスト（evidence management cost）と定義する．

なお，処理 e を含む検証手続を用いる方式では，既存のエンティティを証拠補強者として利用するコスト等が別途必要な場合もある．証拠補強者の役割は E_{TSI} の一貫性確保を目的とする E_{AMP} の保管であり，このようなコストは E_{AMP} の保管コストに含まれるものとする．

4.1.1 検証情報の通信コスト

検証情報の通信コストをタイムスタンプの発行時と検証時に分けて検討する．まず発行時には，発行者がタイムスタンプの一部として E_{TSI} と E_{ORE} を発行依頼者に送るコストと，処理 e を含む検証手続を用いる方式で，発行者が証拠補強者に E_{AMP} を送るコストがかかる．

検証時には，処理 c を含む検証手続を用いる方式で，検証者と発行者がタイムスタンプと検証結果を交信するコストがかかる．処理 e を含む検証手続を用いる方式では，証拠補強者が検証者に E_{AMP} を送るコストがかかる．また，処理 f を含む検証手続を用いる方式では，発行依頼者が検証者に E_{ORE} を送るコストがかかる．

4.1.2 検証情報の保管コスト

検証情報の保管コストを，そのデータを保管するエンティティに分けて検討する．

発行者では，処理 e を含む検証手続を用いる方式で，E_{AMP} を保管するコストがかかるほか，タイムスタンプの一部として E_{TSI} と E_{ORE} を保管するコストがかかる．

証拠補強者では，処理 e を含む検証手続を用いる方式で，発行者から得る E_{AMP} を保管するコストがかかる．

発行依頼者では，タイムスタンプの一部として E_{TSI} と E_{ORE} を保管するコストがかかる．

4.1.3 検証処理に伴うコスト

6 種類の処理を実行するには，それぞれ固有の処理コストがかかる．例えば処理 a では，M のハッシュ値を計算し，H と比較するコストがかかる．

4.2 検討に用いる記号

- $|E_{TSI}|$：1 つの E_{TSI} のデータ量．
- $|E_{AMP}|$：1 つの E_{AMP} のデータ量．E_{AMP} は一定個数のタイムスタンプが発行される度に 1 つ生成されるとし，そのタイムスタンプの個数を k_{AMP} とする．以下の検討では，1 つのタイムスタンプが発行される度にデータ量 $|E_{AMP}|/k_{AMP}$ の E_{AMP} が生成されるとみなす．
- $|E_{ORE}|$：1 つのタイムスタンプを構成する E_{ORE} のデータ量．検証者は，一定数の発行依頼者から E_{ORE} を入手するとし，その人数を k_{ORE} とする．検証者が用いる E_{ORE} のデータ量は $k_{ORE}|E_{ORE}|$ となる．なお，E_{ORE} は E_{TSI} に含まれるので，$|E_{TSI}|>|E_{ORE}|$ となる．
- D_c：処理 c において，発行者から検証者に送信される検証結果のデータ量．
- $|TS|$：1 つのタイムスタンプのデータ量．なお，TS は E_{TSI} を含むので，$|TS|>|E_{TSI}|$ となる．
- C_a：処理 a で，検証者が M のハッシュ値を生成し，タイムスタンプの一部である H と比較するコスト．
- C_b：処理 b において，発行者が $Info_{INT}$ を生成するコスト，および，検証者が，タイムスタンプを構成するデータの一貫性を $Info_{INT}$ によって確認するコスト．例えば，$Info_{INT}$ がディジタル署名の場合，その生成・検証の演算にかかるコスト．
- C_c：処理 c において，発行者が検証対象のタイムスタンプと DB のタイムスタンプを比較するコスト．
- C_d：処理 d で，検証者がタイムスタンプを構成するデータと DB の整合性を E_{TSI} で確認するコスト．
- C_e：処理 e において，発行者が E_{AMP} を生成するコスト，および，検証者が E_{AMP} によって E_{TSI} の一貫性を確認するコスト．
- C_f：処理 f で，検証者が E_{ORE} によって E_{TSI} の一貫性を確認するコスト．

上記各データ量と検証処理に伴うコストは，連鎖型と個別型とによって異なることは言うまでもない．

4.3 検討の前提

各エンティティ間の通信コストと保管コストについては，各コストがそれぞれのデータ量に比例すると仮定し，各データ量の比較によってコストの比較を行うこととする．ただし，処理 e を含む検証手続を用いる方式では，証拠補強者を利用するコスト等の固定的な保管コストが生じる場合も有り得る．以下では，固定

表 3　各検証手続を用いるタイムスタンプ方式における検証情報管理コスト

検証手続	検証手続の適用可能性		通信データ量		保管データ量			検証処理に伴うコスト
	連鎖型	個別型	発行時	検証時	発行者	発行依頼者	証拠補強者	
検証 ab	適用可能	適用可能	$\|E_{TSI}\|$	なし	$\|E_{TSI}\|$	$\|E_{TSI}\|$	なし	$C_a + C_b$
検証 ac				$\|TS\| + D_c$				$C_a + C_c$
検証 ad				なし				$C_a + C_d$
検証 abc				$\|TS\| + D_c$				$C_a + C_b + C_c$
検証 abd				なし				$C_a + C_b + C_d$
検証 ade			$\|E_{TSI}\| + \|E_{AMP}\|/k_{AMP}$	$\|E_{AMP}\|$	$\|E_{TSI}\| + \|E_{AMP}\|/k_{AMP}$		$\|E_{AMP}\|/k_{AMP}$	$C_a + C_d + C_e$
検証 abde								$C_a + C_b + C_d + C_e$
検証 adf		適用不可能	$\|E_{TSI}\|+\|E_{ORE}\|$	$k_{ORE}\|E_{ORE}\|$	$\|E_{TSI}\| + \|E_{ORE}\|$	$\|E_{TSI}\| + \|E_{ORE}\|$	なし	$C_a + C_d + C_f$
検証 abdf								$C_a + C_b + C_d + C_f$
検証 adef			$\|E_{TSI}\| + \|E_{ORE}\| + \|E_{AMP}\|/k_{AMP}$	$\|E_{AMP}\| + k_{ORE}\|E_{ORE}\|$	$\|E_{TSI}\| + \|E_{ORE}\| + \|E_{AMP}\|/k_{AMP}$		$\|E_{AMP}\|/k_{AMP}$	$C_a + C_d + C_e + C_f$
検証 abdef								$C_a + C_b + C_d + C_e + C_f$

・表中の記号については 4.2 を参照.

的なコストを明示的に取り扱わないこととするが，証拠補強者を用いるタイムスタンプ方式を検討する際には，固定的な保管コストも考慮する必要がある．

タイムスタンプ方式の検証手続の中で，安全性に関する条件が同一となった各グループの中で最も処理の数が少ないものを検討対象とする．安全性に関する条件が同一ならば，実装を想定した場合，処理数の少ない検証手続が用いられると考えられるためである．ただし，グループ 1 の検証手続は，安全性の観点から実際に利用されるとは考えにくいため，検討対象から除外する．この結果，ab，ac，ad，abc，abd，ade，adf，abde，abdf，adef，abdef の 11 通りの検証手続を用いる方式を検証対象とする．連鎖型では 11 通りの方式が対象となる一方，個別型では検証 ab，ac，ad，abc，abd，ade，abde を用いる 7 種類の方式が対象となる．

4.4 各方式の検証情報管理コスト（表 3 参照）

4.4.1 検証 ab を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時，発行者がデータ量$|E_{TSI}|$の E_{TSI} をタイムスタンプの一部として発行依頼者に送り，両者が保管．検証処理に伴うコストは C_a+C_b.

4.4.2 検証 ac を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時に，発行者がデータ量$|E_{TSI}|$の E_{TSI} をタイムスタンプの一部として発行依頼者に送り，それを両者が保管．検証時には，検証者と発行者がデータ量$|TS|+D_c$のデータを交信．検証処理に伴うコストは C_a+C_c.

4.4.3 検証 ad を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時に発行者がタイムスタンプの一部としてデータ量$|E_{TSI}|$の E_{TSI} を発行依頼者に送り，それを両者が保管．検証処理に伴うコストは C_a+C_d.

4.4.4 検証 abc を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時に，発行者がタイムスタンプの一部としてデータ量$|E_{TSI}|$の E_{TSI} を発行依頼者に送り，それを両者が保管．検証時には，検証者と発行者がデータ量$|TS|+D_c$ のデータを交信．検証処理に伴うコストは $C_a+C_b+C_c$.

4.4.5 検証 abd を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時に，発行者がタイムスタンプの一部としてデータ量$|E_{TSI}|$の E_{TSI} を発行依頼者に送り，それを両者が保管．検証処理に伴うコストは $C_a+C_b+C_d$.

4.4.6 検証 ade を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時に，発行者はタイムスタンプの一部としてデータ量$|E_{TSI}|$の E_{TSI} を発行依頼者に送付．また，発行者はデータ量$|E_{AMP}|/k_{AMP}$ の E_{AMP} を証拠補強者に送るとみなす．検証時には，証拠補強者がデータ量$|E_{AMP}|$の E_{AMP} を検証者に送付．発行者，発行依頼者，証拠補強者の保管データ量は各々$|E_{TSI}|+|E_{AMP}|/k_{AMP}$，$|E_{TSI}|$，$|E_{AMP}|/k_{AMP}$．検証処理に伴うコストは $C_a+C_d+C_e$.

4.4.7 検証 abde を用いるタイムスタンプ方式

本方式は連鎖型と個別型の両方が想定される．タイムスタンプ発行時に，発行者はタイムスタンプの一部としてデータ量$|E_{TSI}|$の E_{TSI} を発行依頼者に送付．また，発行者はデータ量$|E_{AMP}|/k_{AMP}$ の E_{AMP} を証拠補強者に送るとみなす．検証時に，証拠補強者がデータ量$|E_{AMP}|$の E_{AMP} を検証者に送付．発行者，発行依頼者，証拠補強者の保管データ量は各々$|E_{TSI}|+|E_{AMP}|/k_{AMP}$，$|E_{TSI}|$，$|E_{AMP}|/k_{AMP}$．検証処理に伴うコストは $C_a+C_b+C_d+C_e$.

4.4.8 検証 adf を用いるタイムスタンプ方式

本方式は連鎖型である．タイムスタンプ発行時に，発行者がデータ量$|E_{TSI}|+|E_{ORE}|$の E_{TSI}，E_{ORE} をタイムスタンプの一部として発行依頼者に送付．検証時に，発行依頼者がデータ量 $k_{ORE}|E_{ORE}|$の E_{ORE} を検証者に送付．発行者と発行依頼者の保管データ量は$|E_{TSI}|+|E_{ORE}|$．検証処理に伴うコストは $C_a+C_d+C_f$.

4.4.9 検証 abdf を用いるタイムスタンプ方式

本方式は連鎖型である．タイムスタンプ発行時に，発行者がデータ量$|E_{TSI}|+|E_{ORE}|$の E_{TSI}，E_{ORE} をタイムスタ

ンプの一部として発行依頼者に送付．検証時に，発行依頼者がデータ量 $k_{ORE}|E_{ORE}|$の E_{ORE} を検証者に送付．発行者と発行依頼者の保管データ量は$|E_{TSI}|+|E_{ORE}|$．検証処理に伴うコストは $C_a+C_b+C_d+C_f$．

4.4.10 検証 adef を用いるタイムスタンプ方式

本方式は連鎖型である．タイムスタンプ発行時に，発行者がデータ量$|E_{TSI}|+|E_{ORE}|$の E_{TSI}，E_{ORE} をタイムスタンプの一部として発行依頼者に送付．また，発行者はデータ量$|E_{AMP}|/k_{AMP}$ の E_{AMP} を証拠補強者に送るとみなす．検証時に，証拠補強者が検証者にデータ量$|E_{AMP}|$の E_{AMP} を送り，発行依頼者がデータ量 $k_{ORE}|E_{ORE}|$の E_{ORE} を検証者に送付．発行者，発行依頼者，証拠補強者の保管データ量は各々$|E_{TSI}|+|E_{ORE}|+|E_{AMP}|/k_{AMP}$，$|E_{TSI}|+|E_{ORE}|$，$|E_{AMP}|/k_{AMP}$．検証処理に伴うコストは $C_a+C_d+C_e+C_f$．

4.4.11 検証 abdef を用いるタイムスタンプ方式

本方式は連鎖型である．タイムスタンプ発行時に，発行者がタイムスタンプの一部としてデータ量$|E_{TSI}|+|E_{ORE}|$の E_{TSI}，E_{ORE} を発行依頼者に送付．また，発行者はデータ量$|E_{AMP}|/k_{AMP}$ の E_{AMP} を証拠補強者に送るとみなす．検証時に，証拠補強者が検証者にデータ量$|E_{AMP}|$の E_{AMP} を送り，発行依頼者はデータ量 $k_{ORE}|E_{ORE}|$の E_{ORE} を検証者に送付．発行者，発行依頼者，証拠補強者の保管データ量は各々$|E_{TSI}|+|E_{ORE}|+|E_{AMP}|/k_{AMP}$，$|E_{TSI}|+|E_{ORE}|$，$|E_{AMP}|/k_{AMP}$．検証処理に伴うコストは $C_a+C_b+C_d+C_e+C_f$．

4.5 考察

4.4 では，各検証手続を用いるタイムスタンプ方式の検証情報管理コストの内容を示した．これを基に，各方式の検証手続に別の処理を追加する場合，検証情報管理コストがどのように変化するかについて考察する．

まず，処理 b や処理 d を検証手続に加える場合，通信・保管コストは不変である一方，検証処理に伴うコストがそれぞれ C_b，C_dだけ増加する．

処理 c を検証手続に加える場合，タイムスタンプと検証結果に関する通信コストが追加的に必要となるほか，検証処理に伴うコストも C_cだけ増加する．

処理 e を検証手続に加える場合，検証処理に伴うコストが C_eだけ増加するほか，E_{AMP}の通信・保管コストが必要となる．追加的に必要な通信・保管コストの大きさは k_{AMP} の値と反比例する．また，固定的なコストとして証拠補強者を利用するコスト等が必要となる場合もあり，その際には保管コストが一層増加する．

連鎖型の方式にのみ適用可能な処理 f を検証手続に加える場合，検証処理に伴うコストが C_fだけ増加することに加えて，E_{ORE} の通信コストが必要となる．追加的に必要となる通信コストの大きさは k_{ORE}に比例する．したがって，k_{ORE}を大きくすれば，攻撃者と発行依頼者の結託可能性が低下して安全性が高まると考えられる反面，通信コストが増加することとなる．

以上の考察から，検証手続を構成する処理が増えると，検証情報管理コストも概ね増加する傾向にあり，安全性上最も望ましい検証 abdef を用いる方式では，検証情報管理コストが比較的大きくなるとみられる．

この結果，例えば，高い安全性を確保するために検証 abdef を用いる方式を実装する場合，実用性を少しでも高めるために，安全性を損なうことなく検証情報管理コストを抑える工夫が必要となる．その対応策の 1 つとして，頻繁に利用される通常の検証では例えば検証 abd を利用し，高度な検証が必要な場合にのみ検証 abdef を用いる，という方法が考えられる．このようにすると，通常の検証時における通信コストが不要となるほか，検証処理に伴うコストも C_e+C_fだけ減少し，常に検証 abdef を用いる場合に比べて，検証情報管理コストを削減することが可能となる．

5 おわりに

本稿では，まず，時刻・証拠付タイムスタンプ方式を生成・検証手続によって 48 の方式に分類した上で，宇根・松本[8]の研究成果を基に，各方式におけるタイムスタンプの安全性について検討した．さらに，検証手続に関連するコストとして検証情報管理コストを定義し，各タイムスタンプ方式においてどのような検証情報管理コストが必要となるかを示した．

今後は，宇根・松本[7]が分類した 10 種類のタイムスタンプ方式のうち，これまでに本稿と同様の検討が行われていない時刻・証拠無の方式や時刻付・証拠無の方式について検討を行う方針である．

参考文献

[1] Buldas, A., H. Lipmaa, B. Schoenmakers, "Optimally efficient accountable time-stamping," Proceedings of PKC2000, LNCS 1751, pp. 293-305, 2000.

[2] Cybernetica, "Cuculus: How does it work ?"(http://www.cyber.ee/research/cuc-work.html, 2001 年 1 月 17 日アクセス)

[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. (http://www.fnmt.es/pkits/)

[4] NTT データ，"SecureSeal<テクニカル情報>"，(http://210.144.76.11/technical/tech01.html, 2001 年 1 月 17 日アクセス)

[5] Privador, A.S., "Privador TrueSign™ Technology Overview, Draft", May 25, 2000. (http://gns.privador.com/ts_tech.pdf)

[6] Surety.com, "Secure Time/Data Stamping in a Public Key Infrastructure," (http://www.surety.com/home/pki.pdf, 2001 年 1 月 17 日アクセス)

[7] 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"，CSS2000 予稿集，情報処理学会，pp. 25-30，2000 年 10 月．

[8] 宇根正志，松本勉，"タイムスタンプの検証手続と安全性との関連性"，SCIS2001 予稿集，電子情報通信学会，2001 年 1 月．