(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4788213号
(P4788213)

(45)発行日　平成23年10月5日(2011.10.5)　(24)登録日　平成23年7月29日(2011.7.29)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675B
G09C 1/00 (2006.01)　　H04L 9/00 675D
　　G09C 1/00 640D

請求項の数 2　(全 26 頁)

(21)出願番号　特願2005-204973 (P2005-204973)
(22)出願日　平成17年7月13日 (2005.7.13)
(65)公開番号　特開2007-28015 (P2007-28015A)
(43)公開日　平成19年2月1日 (2007.2.1)
審査請求日　平成20年4月23日 (2008.4.23)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　筧　るみ子
東京都港区赤坂二丁目１７番２２号　富士ゼロックス株式会社内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】タイムスタンプ検証プログラム及びタイムスタンプ検証システム

(57)【特許請求の範囲】
【請求項１】
デジタルデータの生成時刻の認証のためにタイムスタンプ局発行のタイムスタンプの利用者が使用するタイムスタンプ利用側コンピュータを、
タイムスタンプ検証側コンピュータから送られてきた、共通のタイムスタンプが生成された複数のデジタルデータであってそれぞれに乱数が付加された複数のデジタルデータを受信する利用側受信手段、
前記利用側受信手段により受信された複数のデジタルデータのうち、タイムスタンプ検証依頼対象とする検証対象デジタルデータに付加する付加情報を生成する付加情報生成手段、
前記検証対象デジタルデータに前記付加情報を付加して前記タイムスタンプ検証側コンピュータへ送信することによってタイムスタンプの検証を依頼するタイムスタンプ検証依頼手段、
として機能させ、
前記付加情報生成手段は、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータをそれぞれ識別するデータ識別情報に前記タイムスタンプ検証側コンピュータから当該検証対象デジタルデータに付加されて送られてきた乱数を結合させ、その乱数が結合された前記全てのデジタルデータのデータ識別情報を、前記タイムスタンプ検証側コンピュータの公開鍵で暗号化し、その暗号化した前記全てのデジタルデータのデータ識別情報と、前記共通のタイムスタン

プを含むタイムスタンプ情報と、を含めることによって付加情報を生成し、
前記タイムスタンプ利用側コンピュータから送られてくるデジタルデータに付加されたタイムスタンプの検証を行う前記タイムスタンプ検証側コンピュータを、
乱数を生成する乱数生成手段、
前記乱数生成手段が生成した乱数をそれぞれ付加してから前記共通のタイムスタンプが生成された複数のデジタルデータを前記タイムスタンプ利用側コンピュータへ送信するデジタルデータ送信手段、
前記タイムスタンプ利用側コンピュータへ送信するデジタルデータのデータ識別情報に、当該付加された乱数を対応付けして乱数情報記憶手段に登録する登録手段、
前記タイムスタンプ利用側コンピュータから送られてくる前記検証対象デジタルデータであって、前記付加情報が付加された前記検証対象デジタルデータを受信する検証側受信手段、
前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれるタイムスタンプ情報に含まれる前記共通のタイムスタンプを復号することによってダイジェストを生成するタイムスタンプ復号手段、
前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれる暗号化されたデータ識別情報及び乱数を、前記タイムスタンプ検証側コンピュータの公開鍵に対応した秘密鍵で復号し、前記受信手段が受信した前記検証対象デジタルデータのデータ識別情報に対応付けされた乱数を前記乱数記憶手段から取り出し、その取り出した乱数に基づいて、復号したデータ識別情報から乱数を分離することで、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータのデータ識別情報を抽出する抽出手段、
前記抽出手段により抽出されたデータ識別情報それぞれに対応するデジタルデータを取得する取得手段、
前記取得手段が取得したデジタルデータそれぞれから生成したダイジェストと、前記検証対象のデジタルデータから生成したダイジェストと、を結合するダイジェスト生成手段、
前記ダイジェスト生成手段が結合により生成したダイジェストと、前記タイムスタンプ復号手段が生成したダイジェストと、を比較することによってタイムスタンプの検証を行うタイムスタンプ検証手段、
として機能させるタイムスタンプ検証プログラム。
【請求項２】
デジタルデータの生成時刻の認証のためにタイムスタンプ局発行のタイムスタンプの利用者が使用するタイムスタンプ利用側コンピュータと、
前記タイムスタンプ利用側コンピュータから送られてくるデジタルデータに付加されたタイムスタンプの検証を行うタイムスタンプ検証側コンピュータと、
を有し、
前記タイムスタンプ検証側コンピュータから送られてきた、共通のタイムスタンプが生成された複数のデジタルデータであってそれぞれに乱数が付加された複数のデジタルデータを受信する利用側受信手段と、
前記利用側受信手段により受信された複数のデジタルデータのうち、タイムスタンプ検証依頼対象とする検証対象デジタルデータに付加する付加情報を生成する付加情報生成手段と、
前記検証対象デジタルデータに前記付加情報を付加して前記タイムスタンプ検証側コンピュータへ送信することによってタイムスタンプの検証を依頼するタイムスタンプ検証依頼手段と、
を有し、
前記付加情報生成手段は、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータをそれぞれ識別するデータ識別情報に前記タイムスタンプ検証側コンピュータから当該検証対象デジタルデータ

に付加されて送られてきた乱数を結合させ、その乱数が結合された前記全てのデジタルデータのデータ識別情報を、前記タイムスタンプ検証側コンピュータの公開鍵で暗号化し、その暗号化した前記全てのデジタルデータのデータ識別情報と、前記共通のタイムスタンプを含むタイムスタンプ情報と、を含めることによって付加情報を生成し、

前記タイムスタンプ検証側コンピュータは、

乱数を生成する乱数生成手段と、

前記乱数生成手段が生成した乱数をそれぞれ付加してから前記共通のタイムスタンプが生成された複数のデジタルデータを前記タイムスタンプ利用側コンピュータへ送信するデジタルデータ送信手段と、

前記タイムスタンプ利用側コンピュータへ送信するデジタルデータのデータ識別情報に、当該付加された乱数を対応付けして乱数情報記憶手段に登録する登録手段と、

前記タイムスタンプ利用側コンピュータから送られてくる前記検証対象デジタルデータであって、前記付加情報が付加された前記検証対象デジタルデータを受信する検証側受信手段と、

前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれるタイムスタンプ情報に含まれる前記共通のタイムスタンプを復号することによってダイジェストを生成するタイムスタンプ復号手段と、

前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれる暗号化されたデータ識別情報及び乱数を、前記タイムスタンプ検証側コンピュータの公開鍵に対応した秘密鍵で復号し、前記受信手段が受信した前記検証対象デジタルデータのデータ識別情報に対応付けされた乱数を前記乱数記憶手段から取り出し、その取り出した乱数に基づいて、復号したデータ識別情報から乱数を分離することで、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータのデータ識別情報を抽出する抽出手段と、

前記抽出手段により抽出されたデータ識別情報それぞれに対応するデジタルデータを取得する取得手段と、

前記取得手段が取得したデジタルデータそれぞれから生成したダイジェストと、前記検証対象のデジタルデータから生成したダイジェストと、を結合するダイジェスト生成手段と、

前記ダイジェスト生成手段が結合により生成したダイジェストと、前記タイムスタンプ復号手段が生成したダイジェストと、を比較することによってタイムスタンプの検証を行うタイムスタンプ検証手段と、

を有するタイムスタンプ検証システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、タイムスタンプ検証、特に複数のデジタルデータに対して共通したタイムスタンプを生成したときのそのタイムスタンプの取扱いに関する。

【背景技術】

【０００２】

コンピュータ上において電子ファイル等のデジタルデータが作成されると、その作成時刻がデジタルデータの属性情報として設定される。ただ、作成時刻は、本来、変更されるべきでない属性情報であると考えられるが、実際には通常のデータと同様に書き換えることが可能である。つまり、デジタルデータは、過去や未来の時刻を持つデータとして自由自在に作り出すことができてしまうため、デジタルデータが実際にいつ作成されたものであるのか、属性情報のみで保証できないのが現実である。

【０００３】

そこで、現在では、デジタルデータの時刻認証を行うために第三者機関によるタイムスタンプ局が設けられている。すなわち、ユーザがデジタルデータのダイジェストを含むタイムスタンプ要求をタイムスタンプ局へ送信すると、タイムスタンプ局では、送られてき

たダイジェストに時刻情報を付加した後、タイムスタンプ局の秘密鍵を用いてデジタル署名を行った後、署名されたダイジェストを返信する。なお、この返信する情報は、一般に「タイムスタンプトークン」と呼ばれている。そして、ユーザがデジタルデータの、ある時刻での存在を証明したいとき、当該デジタルデータのタイムスタンプが付加されたダイジェストを、タイムスタンプ局においてデジタル署名に用いた秘密鍵に対応した公開鍵を保有するタイムスタンプ局等へ送信することでタイムスタンプの検証を依頼する。依頼を受けたタイムスタンプ局等では、デジタル署名を利用して、送られてきたタイムスタンプの検証を行う。これにより、ユーザは、当該デジタルデータがその時刻にはすでに存在していたことを証明することができる。

【０００４】

以上のように、従来においては、デジタルデータから生成されたダイジェストをタイムスタンプ局に送信することで時刻認証されたタイムスタンプを取得することができる。ただ、タイムスタンプ局からタイムスタンプを取得するには、タイムスタンプ局へダイジェストを送信する必要がある。すなわち、多数のデジタルデータに対してタイムスタンプを取得したい場合、従来においては、全てのデジタルデータのダイジェストを送信しなければならず面倒であった。

【０００５】

そこで、このような問題を解決するために、複数のデジタル文書を結合してダイジェストを生成し、その結合したダイジェストをタイムスタンプ局へ送信するような技術が提案されている（例えば特許文献１）。この従来技術を利用することで、ユーザは、複数のデジタル文書に対して共通した１つのタイムスタンプを取得することができる。従って、複数のデジタル文書と共通の１つのタイムスタンプとの対応関係を自ら管理しておけば、全てのデジタル文書のダイジェストをタイムスタンプ局へ送信する煩わしさから解消されると共に、タイムスタンプの発行に対して従量課金がされる場合には、コストの削減にも貢献することができる。

【０００６】

【特許文献１】特開２００１－１４２３９８号公報
【特許文献２】特開２００３－３３８８１５号公報
【特許文献３】特開２００１－２０９３０８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、従来技術においては、共通したタイムスタンプをデジタル文書に付加した場合、そのデジタル文書のタイムスタンプの検証を個別に行うことができなかった。例えば、３つのデジタル文書Ａ，Ｂ，Ｃに対して共通のタイムスタンプを取得するには、デジタル文書Ａ，Ｂ，Ｃを結合してダイジェストを生成し、その結合したダイジェストをタイムスタンプ局へ送る必要があるが、例えばデジタル文書Ａのタイムスタンプの検証時における復号処理の際には、デジタル文書Ａのみならず、デジタル文書Ａと共に結合ダイジェストを生成した他のデジタル文書Ｂ，Ｃも必要となってくる。つまり、デジタル文書Ａと共に他のデジタル文書Ｂ，Ｃを取り扱わなければデジタル文書Ａのタイムスタンプの検証を行うことができなかった。

【０００８】

本発明は、以上のような課題を解決するためになされたものであり、複数のデジタルデータに共通したタイムスタンプを取得した場合でも、デジタルデータに付加されたタイムスタンプを個別に検証できるようにすることを目的とする。

【課題を解決するための手段】

【００１３】

本発明に係るタイムスタンプ検証プログラムは、デジタルデータの生成時刻の認証のためにタイムスタンプ局発行のタイムスタンプの利用者が使用するタイムスタンプ利用側コンピュータを、タイムスタンプ検証側コンピュータから送られてきた、共通のタイムスタ

ンプが生成された複数のデジタルデータであってそれぞれに乱数が付加された複数のデジタルデータを受信する利用側受信手段、前記利用側受信手段により受信された複数のデジタルデータのうち、タイムスタンプ検証依頼対象とする検証対象デジタルデータに付加する付加情報を生成する付加情報生成手段、前記検証対象デジタルデータに前記付加情報を付加して前記タイムスタンプ検証側コンピュータへ送信することによってタイムスタンプの検証を依頼するタイムスタンプ検証依頼手段として機能させ、前記付加情報生成手段は、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータをそれぞれ識別するデータ識別情報に前記タイムスタンプ検証側コンピュータから当該検証対象デジタルデータに付加されて送られてきた乱数を結合させ、その乱数が結合された前記全てのデジタルデータのデータ識別情報を、前記タイムスタンプ検証側コンピュータの公開鍵で暗号化し、その暗号化した前記全てのデジタルデータのデータ識別情報と、前記共通のタイムスタンプを含むタイムスタンプ情報と、を含めることによって付加情報を生成し、前記タイムスタンプ利用側コンピュータから送られてくるデジタルデータに付加されたタイムスタンプの検証を行う前記タイムスタンプ検証側コンピュータを、乱数を生成する乱数生成手段、前記乱数生成手段が生成した乱数をそれぞれ付加してから前記共通のタイムスタンプが生成された複数のデジタルデータを前記タイムスタンプ利用側コンピュータへ送信するデジタルデータ送信手段、前記タイムスタンプ利用側コンピュータへ送信するデジタルデータのデータ識別情報に、当該付加された乱数を対応付けして乱数情報記憶手段に登録する登録手段、前記タイムスタンプ利用側コンピュータから送られてくる前記検証対象デジタルデータであって、前記付加情報が付加された前記検証対象デジタルデータを受信する検証側受信手段、前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれるタイムスタンプ情報に含まれる前記共通のタイムスタンプを復号することによってダイジェストを生成するタイムスタンプ復号手段、前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれる暗号化されたデータ識別情報及び乱数を、前記タイムスタンプ検証側コンピュータの公開鍵に対応した秘密鍵で復号し、前記受信手段が受信した前記検証対象デジタルデータのデータ識別情報に対応付けされた乱数を前記乱数記憶手段から取り出し、その取り出した乱数に基づいて、復号したデータ識別情報から乱数を分離することで、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータのデータ識別情報を抽出する抽出手段、前記抽出手段により抽出されたデータ識別情報それぞれに対応するデジタルデータを取得する取得手段、

前記取得手段が取得したデジタルデータそれぞれから生成したダイジェストと、前記検証対象のデジタルデータから生成したダイジェストと、を結合するダイジェスト生成手段、前記ダイジェスト生成手段が結合により生成したダイジェストと、前記タイムスタンプ復号手段が生成したダイジェストと、を比較することによってタイムスタンプの検証を行うタイムスタンプ検証手段として機能させる。

【００２０】

また、本発明に係るタイムスタンプ検証システムは、デジタルデータの生成時刻の認証のためにタイムスタンプ局発行のタイムスタンプの利用者が使用するタイムスタンプ利用側コンピュータと、前記タイムスタンプ利用側コンピュータから送られてくるデジタルデータに付加されたタイムスタンプの検証を行うタイムスタンプ検証側コンピュータと、を有し、前記タイムスタンプ検証側コンピュータから送られてきた、共通のタイムスタンプが生成された複数のデジタルデータであってそれぞれに乱数が付加された複数のデジタルデータを受信する利用側受信手段と、前記利用側受信手段により受信された複数のデジタルデータのうち、タイムスタンプ検証依頼対象とする検証対象デジタルデータに付加する付加情報を生成する付加情報生成手段と、前記検証対象デジタルデータに前記付加情報を付加して前記タイムスタンプ検証側コンピュータへ送信することによってタイムスタンプの検証を依頼するタイムスタンプ検証依頼手段と、を有し、前記付加情報生成手段は、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタル

データ以外の全てのデジタルデータをそれぞれ識別するデータ識別情報に前記タイムスタンプ検証側コンピュータから当該検証対象デジタルデータに付加されて送られてきた乱数を結合させ、その乱数が結合された前記全てのデジタルデータのデータ識別情報を、前記タイムスタンプ検証側コンピュータの公開鍵で暗号化し、その暗号化した前記全てのデジタルデータのデータ識別情報と、前記共通のタイムスタンプを含むタイムスタンプ情報と、を含めることによって付加情報を生成し、前記タイムスタンプ検証側コンピュータは、乱数を生成する乱数生成手段と、前記乱数生成手段が生成した乱数をそれぞれ付加してから前記共通のタイムスタンプが生成された複数のデジタルデータを前記タイムスタンプ利用側コンピュータへ送信するデジタルデータ送信手段と、前記タイムスタンプ利用側コンピュータへ送信するデジタルデータのデータ識別情報に、当該付加された乱数を対応付けして乱数情報記憶手段に登録する登録手段と、前記タイムスタンプ利用側コンピュータから送られてくる前記検証対象デジタルデータであって、前記付加情報が付加された前記検証対象デジタルデータを受信する検証側受信手段と、前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれるタイムスタンプ情報に含まれる前記共通のタイムスタンプを復号することによってダイジェストを生成するタイムスタンプ復号手段と、前記受信手段が受信した前記検証対象デジタルデータに付加された付加情報に含まれる暗号化されたデータ識別情報及び乱数を、前記タイムスタンプ検証側コンピュータの公開鍵に対応した秘密鍵で復号し、前記受信手段が受信した前記検証対象デジタルデータのデータ識別情報に対応付けされた乱数を前記乱数記憶手段から取り出し、その取り出した乱数に基づいて、復号したデータ識別情報から乱数を分離することで、前記共通のタイムスタンプが生成された複数のデジタルデータのうち前記検証対象デジタルデータ以外の全てのデジタルデータのデータ識別情報を抽出する抽出手段と、前記抽出手段により抽出されたデータ識別情報それぞれに対応するデジタルデータを取得する取得手段と、前記取得手段が取得したデジタルデータそれぞれから生成したダイジェストと、前記検証対象のデジタルデータから生成したダイジェストと、を結合するダイジェスト生成手段と、前記ダイジェスト生成手段が結合により生成したダイジェストと、前記タイムスタンプ復号手段が生成したダイジェストと、を比較することによってタイムスタンプの検証を行うタイムスタンプ検証手段と、を有するものである。

【発明の効果】

【００２３】

本発明によれば、タイムスタンプ利用側コンピュータにおいて複数のデジタルデータに対して共通のタイムスタンプを取得した場合には、タイムスタンプ検証に必要な他のデジタルデータに関する情報を含む付加情報をデジタルデータに付加するようにしたので、タイムスタンプ検証側コンピュータでは、他のデジタルデータを用いることなく当該デジタルデータに付加されたタイムスタンプを個別に検証することができる。

【発明を実施するための最良の形態】

【００２４】

以下、図面に基づいて、本発明の好適な実施の形態について説明する。

【００２５】

実施の形態１．

図１は、本発明に係るタイムスタンプ検証システムの一実施の形態を示した全体構成図である。図１には、複数台のクライアント１とコンテンツ管理サーバ４とタイムスタンプサーバ７とが公衆網９に接続された構成が示されている。本実施の形態では、タイムスタンプ局発行のタイムスタンプを利用したデジタルデータの時刻認証技術を提供するが、タイムスタンプサーバ７は、タイムスタンプ局に設置されたタイムスタンプ発行用のサーバコンピュータに相当する。本実施の形態では、既存のタイムスタンプサーバをそのまま利用することができる。クライアント１は、デジタルデータに相当するコンテンツの生成時刻の認証のためにタイムスタンプ局発行のタイムスタンプを取得し利用するユーザによって使用されるタイムスタンプ利用側コンピュータに相当する。なお、本実施の形態では、簡易検証と通常検証という２種類のタイムスタンプ検証方法を提供するが、クライアント

１は、簡易検証の場合には、タイムスタンプ利用側コンピュータであるクライアント１からの要求に応じてタイムスタンプの検証を行うタイムスタンプ検証側コンピュータにもなりうる。コンテンツ管理サーバ４は、各クライアント１が取り扱うコンテンツを保持管理するコンピュータであり、また、本実施の形態では、簡易検証及び通常検証において共にタイムスタンプの検証を行うタイムスタンプ検証側コンピュータに相当する。

【００２６】

図２は、本実施の形態におけるタイムスタンプ検証システムのブロック構成図である。図２には、タイムスタンプ利用側コンピュータとして動作するクライアント１と、タイムスタンプ検証側コンピュータとして動作するコンテンツ管理サーバ４とが、それぞれ示されている。

【００２７】

クライアント１は、コンテンツ取得部１２、タイムスタンプ生成依頼処理部１４、タイムスタンプ検証依頼処理部１６及び表示部１８を有している。コンテンツ取得部１２は、タイムスタンプの付加対象とするコンテンツをコンテンツ管理サーバ４から取得し、コンテンツ保存部３４に保存する。タイムスタンプ生成依頼処理部１４は、ダイジェスト生成部２０、ダイジェスト送信部２２及びタイムスタンプ取得部２４を有し、タイムスタンプの生成依頼要求をコンテンツ管理サーバ４に送信することによって複数のコンテンツに共通して付加するタイムスタンプを取得する。ダイジェスト生成部２０は、ハッシュ関数を用いてコンテンツからダイジェストを生成する。ダイジェスト送信部２２は、各コンテンツから生成されたダイジェストをコンテンツ管理サーバ４へ送信することでタイムスタンプの生成依頼要求を出す。タイムスタンプ取得部２４は、送信した生成依頼要求に応じてコンテンツ管理サーバ４がタイムスタンプ局から取得したタイムスタンプ情報を取得し、タイムスタンプ保持テーブル３６に登録する。タイムスタンプ情報には、タイムスタンプトークンに含まれるタイムスタンプ及びタイムスタンプの生成時刻が含まれており、タイムスタンプ保持テーブル３６には、取得したタイムスタンプ情報に、当該タイムスタンプが付加される複数のコンテンツを識別する情報、本実施の形態ではコンテンツＩＤを対応付けして設定登録される。

【００２８】

タイムスタンプ検証依頼処理部１６は、付加情報生成部２６、検証依頼部２８及び検証結果取得部３０を有し、コンテンツに付加されたタイムスタンプの検証をコンテンツ管理サーバ４に依頼する。タイムスタンプ検証依頼処理部１６に含まれる付加情報生成部２６は、コンテンツ管理サーバ４におけるタイムスタンプ検証に必要な付加情報を生成する。付加情報生成部２６に含まれる他コンテンツ情報生成部３２は、タイムスタンプを付加する各コンテンツに対して、当該コンテンツと共にタイムスタンプが生成された他のコンテンツに関する情報を生成する。検証依頼部２８は、検証対象のタイムスタンプが付加されたコンテンツに、付加情報生成部２６が生成した付加情報を付加して構成されるコンテンツ情報をコンテンツ管理サーバ４へ送信することでタイムスタンプ検証を依頼する。検証結果取得部３０は、コンテンツ管理サーバ４におけるタイムスタンプ検証の結果をコンテンツ管理サーバ４から取得する。表示部１８は、検証結果取得部３０が取得した検証結果を表示する。クライアント１が有する各構成要素１２～１８の処理機能は、当該処理機能を発揮するタイムスタンプ検証プログラムと、クライアント１を構成するハードウェアとの協調動作により実現される。

【００２９】

一方、コンテンツ管理サーバ４は、コンテンツ配信部４２、タイムスタンプ取得処理部４４及びタイムスタンプ検証処理部４６を有している。コンテンツ配信部４２は、コンテンツデータベース６８に格納されているコンテンツを配信要求元のクライアント１へダウンロードする。タイムスタンプ取得処理部４４は、ダイジェスト取得部４８、タイムスタンプ要求部５０、タイムスタンプ取得部５２及びタイムスタンプ通知部５４を有し、クライアント１からのタイムスタンプの生成依頼要求に応じてタイムスタンプサーバ７からタイムスタンプを取得し、要求元のクライアント１へ返信する。ダイジェスト取得部４８は

、クライアント１からのタイムスタンプの生成依頼要求を受け付ける。クライアント１から送られてくる生成依頼要求には、タイムスタンプを付加する複数のコンテンツの各ダイジェストが含まれているので、タイムスタンプ要求部５０は、各ダイジェストからハッシュ関数Ｈを用いて単一の結合ダイジェストを生成し、この結合ダイジェストを含むタイムスタンプ要求をタイムスタンプサーバ７へ送信する。タイムスタンプ取得部５２は、タイムスタンプ要求に応じてタイムスタンプサーバ７が生成したタイムスタンプトークンを受け取ると共に、タイムスタンプトークンに含まれているタイムスタンプ情報、すなわちタイムスタンプ及びタイムスタンプ生成時間情報である生成時刻に、タイムスタンプを付加する複数のコンテンツの識別情報を対応付けしてタイムスタンプ管理テーブル７０に登録する。タイムスタンプ通知部５４は、タイムスタンプ及びその生成時刻を含むタイムスタンプ情報を生成依頼要求元のクライアント１へ送信する。

【００３０】

タイムスタンプ検証処理部４６は、検証依頼受付部５８、コンテンツ読出部６０、ダイジェスト生成部６２、タイムスタンプ検証部６４及び検証結果通知部６６を有し、クライアント１からの要求に応じてコンテンツに付加されたタイムスタンプの検証を行う。検証依頼受付部５８は、クライアント１から送られてくるタイムスタンプの検証依頼要求を受け付ける。この要求には、検証対象のタイムスタンプを含む付加情報が付加されたコンテンツが含まれている。コンテンツ読出部６０は、通常検証の際に必要なコンテンツをコンテンツデータベース６８から読み出す。ダイジェスト生成部６２は、ハッシュ関数を用いてコンテンツからダイジェストを生成する。ダイジェスト生成部６２が使用するハッシュ関数は、各クライアント１が使用するハッシュ関数と同一である。タイムスタンプ検証部６４は、クライアント１から送られてきたコンテンツ及び付加情報から２種類の方法で生成した各ダイジェストを比較することでタイムスタンプの検証を行う。検証結果通知部６６は、タイムスタンプ検証部６４における検証結果をコンテンツ送信元のクライアント１へ通知する。コンテンツ管理サーバ４が有する各構成要素４２～４６の処理機能は、当該処理機能を発揮するタイムスタンプ検証プログラムと、コンテンツ管理サーバ４を構成するハードウェアとの協調動作により実現される。

【００３１】

次に、本実施の形態における動作について説明するが、その前に動作の説明に用いる各種記号、変数等について定義する。

【００３２】

まず、タイムスタンプが付加されるメッセージデータとして用いるコンテンツをＣｘ（ｘ＝１，２，・・・Ｎ）と定義する。また、各コンテンツＣｘのタイムスタンプ生成対象領域をＳｘ、タイムスタンプ情報を含む付加情報などのＳｘ以外の情報を格納するタイムスタンプ情報領域をＥｘとする。タイムスタンプ生成対象領域Ｓｘというのは、コンテンツを構成するデータのうちタイムスタンプ生成の際に必要なダイジェストの生成に用いるデータを含む領域である。タイムスタンプ情報領域Ｅｘというのは、ダイジェストに付加する情報の格納領域であり、本実施の形態では、タイムスタンプ情報を含む付加情報を格納する領域に相当する。クライアント１は、コンテンツＣｘ毎に、ダイジェストの生成に用いるデータを含む署名対象領域Ｓｘと、署名検証のために必要な情報を含む署名情報領域Ｅｘとを組にしてコンテンツ管理サーバ４へ送信することになる。また、コンテンツのダイジェストを生成するためにクライアント１及びコンテンツ管理サーバ４が持つハッシュ関数をｆ、タイムスタンプ取得の際にコンテンツ管理サーバ４が使用するハッシュ関数をＨ、各コンテンツを識別する情報として用いるコンテンツＩＤをＩＤｘ、署名関数をＥｎｃ（ｓｉｇｎｋｅｙ，ｄａｔａ）、検証関数をＤｅｃ（ｖｅｒｉｆｙｋｅｙ，ｄａｔａ）、コンテンツ管理サーバ４の公開鍵をＥｓ、コンテンツ管理サーバ４の秘密鍵をＤｓ、タイムスタンプサーバ７の公開鍵をＥｔ、タイムスタンプサーバ７の秘密鍵をＤｔ、タイムスタンプ生成時刻をＴｔ、タイムスタンプトークンをＴＳＴ（ｔｉｍｅ，ＳｉｇＶａｌｕｅ）と定義する。なお、署名関数及び検証関数に指定するｓｉｇｎｋｅｙ、ｖｅｒｉｆｙｋｅｙには暗号化／復号に用いる鍵が、ｄａｔａには暗号化／復号されるデータが、そ

れぞれ設定される。また、タイムスタンプトークンに指定するｔｉｍｅにはタイムスタンプ生成時刻が、ＳｉｇＶａｌｕｅにはタイムスタンプが、それぞれ設定される。

【００３３】

以上のように定義したデータや関数を用いて、本実施の形態におけるタイムスタンプ検証について説明する。タイムスタンプ検証は、タイムスタンプの生成処理とタイムスタンプの検証処理とに大別できる。まず最初に、タイムスタンプ生成処理についてクライアント１における処理を示した図３及びコンテンツ管理サーバ４における処理を示した図４を用いて説明する。

【００３４】

クライアント１のコンテンツ取得部１２は、コンテンツのダウンロード要求をコンテンツ管理サーバ４へ発すると、コンテンツ管理サーバ４のコンテンツ配信部４２は、クライアント１からの要求に応じてタイムスタンプ付加対象のＮ個のコンテンツＣｘ（ｘ＝１～Ｎ）を当該クライアント１へ送信する（ステップ２１１）。コンテンツ取得部１２は、このようにしてＮ個のコンテンツＣｘを取得すると、これらをコンテンツ保存部３４に保存する（ステップ１１１）。コンテンツＣｘをいったん保存するようにしたのは、タイムスタンプの検証の際にコンテンツＣｘが必要であり、またタイムスタンプの検証がタイムスタンプを取得してしばらく時間が経過してから行われると考えられるからである。後述するタイムスタンプ保持テーブル３６でタイムスタンプ情報を保持するのも同じ理由による。なお、取得した各コンテンツＣｘ（ｘ＝１～Ｎ）のＩＤは、それぞれＩＤｘ（ｘ＝１～Ｎ）とする。

【００３５】

タイムスタンプ生成依頼処理部１４におけるダイジェスト生成部２０は、取得された各コンテンツＩＤｘの署名対象領域Ｓｘに含まれるデータからハッシュ関数ｆを用いてＮ個のダイジェストｆ（Ｓｘ）を生成する（ステップ１１２）。続いて、ダイジェスト送信部２２は、コンテンツＣｘから生成されたダイジェストｆ（Ｓｘ）をコンテンツ管理サーバ４へ送信することでタイムスタンプの生成依頼要求を出す（ステップ１１３）。

【００３６】

コンテンツ管理サーバ４において、ダイジェスト取得部４８がクライアント１からのタイムスタンプの生成依頼要求を受信すると（ステップ２１２）、タイムスタンプ要求部５０は、生成依頼要求に含まれている複数のダイジェストを結合する。この結合ダイジェストＦは、次のように表すことができる。

【数１】

$$F = \sum_{X=1}^{N} f(S_X)$$

【００３７】

そして、タイムスタンプ要求部５０は、この結合ダイジェストＦからハッシュ関数Ｈを用いて単一のダイジェストＨ（Ｆ）を生成し（ステップ２１３）、このダイジェストＨ（Ｆ）を含むタイムスタンプ要求をタイムスタンプサーバ７へ送信する（ステップ２１４）。

【００３８】

タイムスタンプサーバ７は、コンテンツ管理サーバ４から送られてきたダイジェストに、信頼できる時間源から取得した現在時刻をタイムスタンプ生成時刻として付加し、これに自己の秘密鍵Ｄｔを用いて署名を行い、タイムスタンプトークンを生成する。そして、要求元のコンテンツ管理サーバ４へタイムスタンプトークンを返信する。なお、署名ＴＳＶａｌｕｅ及びタイムスタンプトークンＴＳＴｏｋｅｎを式にて表すと、次のように表すことができる。

ＴＳＶａｌｕｅ＝Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（Ｆ））

ＴＳＴｏｋｅｎ＝ＴＳＴ（Ｔｔ，ＴＳＶａｌｕｅ）

【００３９】

コンテンツ管理サーバ４において、タイムスタンプ取得部５２は、タイムスタンプ要求に応じてタイムスタンプサーバ７が生成したタイムスタンプトークンを受け取ると共に（ステップ２１５）、タイムスタンプトークンに含まれているタイムスタンプ情報、すなわちタイムスタンプＴＳＶａｌｕｅ及びタイムスタンプ生成時刻Ｔｔに、タイムスタンプを付加する複数のコンテンツの識別情報ＩＤｘを対応付けしてタイムスタンプ管理テーブル７０に登録する（ステップ２１６）。なお、タイムスタンプ情報には、どのコンテンツに対するタイムスタンプかを特定できる情報が付加すればよいので、必ずしも識別情報ＩＤｘでなくてもよい。本実施の形態では、タイムスタンプ管理テーブル７０を用いる必要はないが、管理サーバの一機能としてタイムスタンプを保持管理する。タイムスタンプ通知部５４は、タイムスタンプ及びその生成時刻を含むタイムスタンプ情報を生成依頼要求元のクライアント１に通知する（ステップ２１７）。

【００４０】

クライアント１において、タイムスタンプ取得部２４は、生成依頼要求に応じてコンテンツ管理サーバ４から送られてくるタイムスタンプ情報を受信すると、タイムスタンプ情報、すなわちタイムスタンプＴＳＶａｌｕｅ及びタイムスタンプ生成時刻Ｔｔに、タイムスタンプを付加する複数のコンテンツの識別情報ＩＤｘを対応付けしてタイムスタンプ保持テーブル３６に登録する（ステップ１１４）。なお、タイムスタンプ情報には、どのコンテンツに対するタイムスタンプかを特定できる情報が付加すればよいので、必ずしも識別情報ＩＤｘでなくてもよい。

【００４１】

本実施の形態においては、以上のようにして複数のコンテンツに対して共通した１つのタイムスタンプを生成することができる。これにより、コンテンツ個々にタイムスタンプの生成依頼をする必要がないので、便利であり、また、コスト削減を図ることができる。

【００４２】

続いて、タイムスタンプ検証処理について説明するが、本実施の形態では、前述したように簡易検証と通常検証という２種類のタイムスタンプ検証方法を提供する。最初に簡易検証について、タイムスタンプ検証依頼を行うクライアント１における処理を示した図５及びクライアント１からの依頼に応じてタイムスタンプ検証を行うコンテンツ管理サーバ４における処理を示した図６を用いて説明する。

【００４３】

共通してタイムスタンプが付加されたコンテンツＩＤがそれぞれＩＤｘ（ｘ＝１～Ｎ）であるＮ個のコンテンツＣｘ（ｘ＝１～Ｎ）のうち、いずれかのコンテンツのタイムスタンプの検証を依頼したいとする。なお、以下で説明する処理は、全てのコンテンツＣｘに対して同じなので、ここでは、$ＩＤ_1$のコンテンツ$Ｃ_1$を代表させて説明する。

【００４４】

このとき、タイムスタンプ検証依頼処理部１６は、全てのコンテンツＣｘをコンテンツ保存部３４から読み出し、検証依頼のためにコンテンツ管理サーバ４へ送信するコンテンツ$Ｃ_1$に対して付加する付加情報を付加情報生成部２６に生成させる（ステップ１１５）。

【００４５】

すなわち、付加情報生成部２６における他コンテンツ情報生成部３２は、$Ｃ_1$以外の他のコンテンツに関する情報として、$Ｃ_1$と共にタイムスタンプが生成された他のコンテンツＣｘ（ｘ＝２～Ｎ）の識別情報｛$ＩＤ_2$，$ＩＤ_3$，$ＩＤ_4$，・・・，$ＩＤ_N$｝と、当該他のコンテンツのダイジェスト｛ｆ（$Ｓ_2$），ｆ（$Ｓ_3$），ｆ（$Ｓ_4$），・・・，ｆ（$Ｓ_N$）｝とを生成する。なお、他のコンテンツのダイジェストｆ（Ｓｘ）（ｘ＝２～Ｎ）は、各コンテンツＩＤｘの署名対象領域Ｓｘに含まれるデータからハッシュ関数ｆを用いて生成される。なお、$ＩＤ_2$のコンテンツ$Ｃ_2$であれば、$Ｃ_2$と共に一括署名が生成された他のコンテンツの識別情報｛$ＩＤ_1$，$ＩＤ_3$，$ＩＤ_4$，・・・，$ＩＤ_N$｝と、当該他のコンテンツのダイジェスト｛ｆ（$Ｓ_1$），ｆ（$Ｓ_3$），ｆ（$Ｓ_4$），・・・，ｆ（$Ｓ_N$）｝とが生成されることになる。更に、付加情報生成部２６は、タイムスタンプ保持テーブル

３６からコンテンツＣｘ（ｘ＝１～Ｎ）に共通したタイムスタンプ情報を取り出し、付加情報に含める。以上のようにして生成された付加情報は、次のように表すことができる。

【００４６】

E_1＝（｛ID_2，ID_3，ID_4，・・・，ID_N｝，｛ｆ（S_2），ｆ（S_3），ｆ（S_4），・・・，ｆ（S_N）｝，Ｔｔ，ＴＳＶａｌｕｅ）

【００４７】

検証依頼部２８は、検証対象となるコンテンツC_1に上記付加情報を付加してコンテンツ管理サーバ４へ送信することで、タイムスタンプ検証を依頼する（ステップ１１６）。

【００４８】

なお、本実施の形態では、他のコンテンツのダイジェストｆ（Ｓｘ）（ｘ＝２～Ｎ）を付加情報に含める必要があるため、タイムスタンプの検証依頼を行う際に、タイムスタンプ検証依頼処理部１６において該当するダイジェストを生成するように説明したが、各コンテンツのダイジェストは、タイムスタンプ生成依頼時にも生成しているので、このときに生成したダイジェストをタイムスタンプ保持テーブル３６で保管しておき、タイムスタンプ検証依頼時に再利用するようにしてもよい。

【００４９】

コンテンツ管理サーバ４において、タイムスタンプ検証処理部４６における検証依頼受付部５８がクライアント１から発せられたタイムスタンプ生成依頼要求を受信すると（ステップ２２１）、タイムスタンプ検証部６４は、受信したコンテンツC_1の付加情報に含まれているタイムスタンプＴＳＶａｌｕｅを、タイムスタンプサーバ７の公開鍵Ｅｔを用いて復号することでダイジェストを生成する（ステップ２２２）。このダイジェストの生成は、検証関数を用いるので、Ｄｅｃ（Ｅｔ，ＴＳＶａｌｕｅ）と表すことができるが、復号されたＴＳＶａｌｕｅは、Ｔｔ＋Ｈ（Ｆ）と表すことができる。

【００５０】

一方、ダイジェスト生成部６２は、クライアント１から送られてきたコンテンツC_1からダイジェストを生成する（ステップ２２４）。このダイジェストの生成についてより厳密に言うと、ダイジェスト生成部６２は、ハッシュ関数ｆを用いてコンテンツC_1の署名対象領域S_1に含まれているデータからダイジェストｆ（S_1）を生成する。ここで、コンテンツC_1以外のコンテンツＣｘ（ｘ＝２～Ｎ）のダイジェストｆ（Ｓｘ）（ｘ＝２～Ｎ）は、コンテンツC_1の付加情報に含まれているので、ダイジェスト生成部６２は、ｆ（S_1）とｆ（Ｓｘ）（ｘ＝２～Ｎ）、すなわち共通のタイムスタンプが生成された全てのコンテンツＣｘ（ｘ＝１～Ｎ）のダイジェストを結合して結合ダイジェストＦを生成する（ステップ２２４）。

【００５１】

タイムスタンプ検証部６４は、タイムスタンプ検証を行うダイジェストを完成させるため、結合ダイジェストＦからハッシュ関数Ｈを用いてダイジェストＨ（Ｆ）を生成し、これに受信した付加情報に含まれているタイムスタンプ生成時刻Ｔｔを付加してＴｔ＋Ｈ（Ｆ）を得る。

【００５２】

以上のようにして比較対象のダイジェストが生成されると、２つのダイジェスト、すなわち、タイムスタンプの復号により得られたダイジェストＤｅｃ（Ｅｔ，ＴＳＶａｌｕｅ）、すなわちＴｔ＋Ｈ（Ｆ）と、コンテンツ管理サーバ４にて生成したダイジェストＴｔ＋Ｈ（Ｆ）とを比較することで、コンテンツC_1に付加されたタイムスタンプを検証する（ステップ２２５）。以上のように、比較対象のダイジェストは、共にＴｔ＋Ｈ（Ｆ）と表され、改竄されていなければ、検証に成功するはずである。

【００５３】

なお、フローチャートでは、受信したタイムスタンプを復号してダイジェストを生成する処理を、ダイジェスト生成部６２が結合ダイジェストを生成する処理より先に行うように説明したが、この処理の順番は逆でもいし、同時並行して行うようにしてもよい。

【００５４】

検証結果通知部６６は、以上のようにしてコンテンツＣ$_1$に付加されたタイムスタンプの検証結果を検証依頼元のクライアント１へ通知する（ステップ２２６）。

【００５５】

クライアント１において、検証結果取得部３０がコンテンツ管理サーバ４から通知されてきた検証結果を取得すると（ステップ１１７）、表示部１８は、クライアント１のディスプレイに表示することで（ステップ１１８）、ユーザにタイムスタンプの検証結果を知らせる。

【００５６】

本実施の形態におけるタイムスタンプの簡易検証は、以上のようにして行うが、本実施の形態においては、コンテンツ個々のタイムスタンプ検証の際に必要な他のコンテンツのダイジェストを、当該コンテンツの付加情報に含めるようにした。つまり、タイムスタンプの生成の際に用いた他のコンテンツのダイジェスト、例えば、コンテンツＣ$_1$に付加されたタイムスタンプの検証の場合であれば、コンテンツＣｘ（ｘ＝２～Ｎ）のダイジェストｆ（Ｓｘ）（ｘ＝２～Ｎ）をコンテンツＣ$_1$の付加情報に含めるようにしたので、タイムスタンプ検証を行うコンテンツ管理サーバ４は、他のコンテンツＣｘ（ｘ＝２～Ｎ）からダイジェストを生成する必要がない。すなわち、コンテンツ管理サーバ４は、コンテンツＣ$_1$に付加されたタイムスタンプの検証を、他のコンテンツＣｘ（ｘ＝２～Ｎ）がなくても個別に行うことができる。

【００５７】

続いて、通常検証について説明するが、タイムスタンプ件書依頼側のクライアント１における処理は、簡易検証と同じなので説明を省略する。ここでは、コンテンツ管理サーバ４におけるタイムスタンプ検証時処理について図７に示したフローチャートを用いて説明する。なお、簡易検証と同じ処理には同じステップ番号を付け、説明を適宜省略又は簡略する。

【００５８】

タイムスタンプ検証側であるコンテンツ管理サーバ４において、検証依頼受付部５８がタイムスタンプ生成依頼要求を受信すると（ステップ２２１）、タイムスタンプ検証部６４は、受信したコンテンツＣ$_1$の付加情報に含まれているタイムスタンプを復号してダイジェストＴｔ＋Ｈ（Ｆ）を生成する（ステップ２２２）。

【００５９】

一方、ダイジェスト生成部６２は、コンテンツＣ$_1$の付加情報に含まれている他のコンテンツの識別情報｛ＩＤ$_2$，ＩＤ$_3$，ＩＤ$_4$，・・・，ＩＤ$_N$｝を取り出す。そして、ダイジェスト生成部６２は、コンテンツ読出部６０に取り出したコンテンツＩＤを渡す。コンテンツ読出部６０は、そのコンテンツＩＤをキーにして当該コンテンツをコンテンツデータベース６８から読み出す。なお、コンテンツ管理サーバ４がコンテンツデータベース６８を保有していなければ、コンテンツ読出部６０は、ネットワーク経由で外部から取得してくることになる。これにより、ダイジェスト生成部６２は、ハッシュ関数ｆを用いて簡易検証と同様にクライアント１から送られてきたコンテンツＣ$_1$からダイジェストｆ（Ｓ$_1$）を生成すると共に、コンテンツデータベース６８から読み出したその他のコンテンツＣｘ（ｘ＝２～Ｎ）からダイジェストｆ（Ｓｘ）（ｘ＝２～Ｎ）を生成する（ステップ２２７）。このようにして、共通のタイムスタンプを生成した全てのコンテンツのダイジェストを取得することができるので、これらのダイジェストを結合して結合ダイジェストＦを生成する（ステップ２２８）。この結合ダイジェストは、簡易検証と同じ内容になる。

【００６０】

この後の処理は、簡易検証と同じであり、タイムスタンプ検証部６４は、タイムスタンプ検証を行うダイジェストを完成させるため、結合ダイジェストＦからダイジェストＨ（Ｆ）を生成し、これに受信した付加情報に含まれているタイムスタンプ生成時刻Ｔｔを付加してＴｔ＋Ｈ（Ｆ）を得る。

【００６１】

以上のようにして比較対象のダイジェストが生成されると、タイムスタンプ検証部６４は、タイムスタンプの復号により得られたダイジェストＴｔ＋Ｈ（Ｆ）と、コンテンツ管理サーバ４にて生成したダイジェストＴｔ＋Ｈ（Ｆ）とを比較することで、コンテンツ$Ｃ_{1}$に付加されたタイムスタンプを検証する（ステップ２２５）。そして、検証結果通知部６６は、コンテンツ$Ｃ_{1}$に付加されたタイムスタンプの検証結果を検証依頼元のクライアント１へ通知する（ステップ２２６）。なお、検証結果の通知、表示の処理に関しては、簡易検証と同じなので省略する。

【００６２】

本実施の形態におけるタイムスタンプの通常検証は、以上のようにして行うが、通常検証も簡易検証と同様に複数のコンテンツに対して共通したタイムスタンプを生成した場合でもコンテンツに付加されたタイムスタンプの検証を、コンテンツ毎に行うことができる。

【００６３】

なお、上記説明では、コンテンツ管理サーバ４は、クライアント１へコンテンツを送信し、クライアント１にて生成されたダイジェストを受け取るように処理するが、通常検証の場合、コンテンツ管理サーバ４は、コンテンツデータベース６８により各コンテンツを持っているので、共通したタイムスタンプを生成するコンテンツを特定しうる情報、例えばコンテンツＩＤを受け取り、コンテンツ管理サーバ４側で各コンテンツのダイジェストを生成するようにしてもよい。

【００６４】

また、コンテンツ管理サーバ４は、結合対象のダイジェストをクライアント１から受け取り、コンテンツ管理サーバ４にて結合ダイジェストＦを生成しているっているが、クライアント１側にて結合ダイジェストＦを生成させ、それを受け取るようにしてもよい。

【００６５】

本実施の形態においては、コンテンツ管理サーバ４において、付加情報に含まれるタイムスタンプを復号して生成したダイジェストと比較するダイジェストを生成する過程において、複数のコンテンツのダイジェストを生成するようにしたが、簡易検証と通常検証とでは、タイムスタンプを含む付加情報が付加されたコンテンツ（以下、「被付加コンテンツ」ともいう、前述した例で言うとコンテンツ$Ｃ_{1}$）以外のコンテンツＣｘ（ｘ＝２～Ｎ）のダイジェストの取得方法が異なっている。すなわち、簡易検証では、被付加コンテンツ以外の他のコンテンツのダイジェストを、被付加コンテンツの付加情報から取得するのに対し、通常検証では、当該被付加コンテンツの付加情報から取得した他のコンテンツのＩＤをキーにしてコンテンツを取得し、そして他のコンテンツのダイジェストを自ら生成する。この他のコンテンツのダイジェストの取得方法の違いにより、コンテンツ管理サーバ４で実施される各検証方法は、以下のような特徴を有していることになる。

【００６６】

まず、通常検証の場合、ダイジェストの生成のためにコンテンツそのものが必要になってくるので、コンテンツそのものを保持管理するコンテンツ管理サーバ４にとっては、外部からコンテンツを取得することなく通常検証を実施することができる。つまり、通常検証の場合は、付加情報にコンテンツＩＤを含めておけばよいので、ダイジェストそのものが改竄される可能性がない。これにより、タイムスタンプ検証の確度を向上させることができる。

【００６７】

これに対し、簡易検証は、コンテンツのダイジェストを直接受け取るため、コンテンツそのものを必要としない。従って、コンテンツ管理サーバ４のみならずコンテンツそのものを保持管理しないクライアント１においても、簡易検証であればタイムスタンプの検証を行うことができる。つまり、クライアント１が簡易検証を行う場合、そのクライアント１に、図２に示したコンテンツ管理サーバ４からタイムスタンプ検証処理部４６を持たせることで、クライアント１にもタイムスタンプ検証側のコンピュータとして動作させることができる。

【００６８】
なお、コンテンツの付加情報には、他のコンテンツに関する情報として、他のコンテンツのＩＤと他のコンテンツのダイジェストとが含まれている。簡易検証と通常検証の各処理の説明から明らかなように、他のコンテンツに関する情報として、簡易検証では他のコンテンツのダイジェストを、通常検証では他のコンテンツのＩＤをそれぞれ使用し、他方の情報は使用していない。従って、クライアント１は、簡易検証を実施することが明らかであるならば、付加情報に他のコンテンツのＩＤを含める必要はない。一方、通常検証を実施することが明らかであるならば、付加情報に他のコンテンツのダイジェストを含める必要はない。ただ、本実施の形態では、タイムスタンプ検証側コンピュータが、自己の構成等によっていずれの検証方法を適宜使用できるように、他のコンテンツに関する情報として他のコンテンツのＩＤとダイジェストとの双方の情報を含めるようにした。

【００６９】
次に、前述したタイムスタンプの生成処理及び検証処理について具体例を用いて説明する。なお、処理の内容は、上記と同じなので適宜簡略化して説明する。ここでは、タイムスタンプを生成するコンテンツＩＤがそれぞれＩＤ１，ＩＤ２，ＩＤ３である３つのコンテンツＣ１，Ｃ２，Ｃ３を取り扱う場合を例にして説明する。また、各コンテンツＣ１～Ｃ３の署名対象領域をＳ１，Ｓ２，Ｓ３、署名情報領域をＥ１，Ｅ２，Ｅ３とする。まず、タイムスタンプ生成時における処理から説明するが、クライアント１における処理内容は、簡易検証と通常検証とで同じである。

【００７０】
クライアント１において、上記３つのコンテンツをコンテンツ管理サーバ４からダウンロードすることで取得すると（ステップ１１１）、ハッシュ関数ｆを用いてダイジェストｆ（Ｓ１），ｆ（Ｓ２），ｆ（Ｓ３）をそれぞれ生成し（ステップ１１２）、コンテンツ管理サーバ４へ送信することでタイムスタンプの生成依頼要求を出す（ステップ１１３）。

【００７１】
コンテンツ管理サーバ４は、クライアント１からのタイムスタンプの生成依頼要求を受信すると（ステップ２１２）、タイムスタンプ要求部５０は、生成依頼要求に含まれている複数のダイジェストＦ（＝ｆ（Ｓ１＋Ｓ２＋Ｓ３）を結合し、ハッシュ関数Ｈを用いてダイジェストＨ（Ｆ）生成し（ステップ２１３）、タイムスタンプサーバ７へ送信する（ステップ２１４）。そして、タイムスタンプサーバ７から送られてきたタイムスタンプトークンを受信すると、タイムスタンプ情報、すなわちＴｔとＨ（Ｆ）をクライアント１へ通知する（ステップ２１７）。

【００７２】
このようにして、クライアント１は、コンテンツＣ１～Ｃ３に共通したタイムスタンプを得ることができる。続いて、タイムスタンプ検証時における処理のうち簡易検証について説明するが、ここでは、コンテンツＣ１に付加されたタイムスタンプの検証を行う場合を例にして説明する。

【００７３】
タイムスタンプ検証依頼処理部１６の付加情報生成部２６は、ハッシュ関数ｆを用いて他のコンテンツＣ２，Ｃ３のダイジェストｆ（Ｓ２），ｆ（Ｓ３）をそれぞれ生成し、他のコンテンツＣ２，Ｃ３の識別情報｛ＩＤ２，ＩＤ３｝と、ダイジェスト｛ｆ（Ｓ２），ｆ（Ｓ３）｝とを生成する。更に、タイムスタンプ情報をタイムスタンプ保持テーブル３６から取り出して、付加情報を生成するが、この付加情報は、次のようになる。
Ｅ１＝（｛ＩＤ２，ＩＤ３｝），｛ｆ（Ｓ２），ｆ（Ｓ３）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

【００７４】
なお、参考までにコンテンツＣ２，Ｃ３の付加情報は、次のようになる。
Ｅ２＝（｛ＩＤ３，ＩＤ１｝），｛ｆ（Ｓ３），ｆ（Ｓ１）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

Ｅ３＝（｛ＩＤ１，ＩＤ２｝），｛ｆ（Ｓ１），ｆ（Ｓ２）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

【００７５】

このようにして生成された付加情報Ｅ１は、コンテンツＣ１を格納する領域Ｓ１に付加されてタイムスタンプ生成依頼要求としてコンテンツ管理サーバ４へ送信される（ステップ１１６）。なお、簡易検証の場合のタイムスタンプ検証側コンピュータとして、ここではコンテンツ管理サーバ４を例にしているが、クライアント１でもよいことは前述したとおりである。

【００７６】

コンテンツ管理サーバ４において、クライアント１から発せられたタイムスタンプ生成依頼要求を受信すると（ステップ２２１）、タイムスタンプ検証部６４は、受信したコンテンツＣ１の付加情報に含まれているタイムスタンプＥｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を、タイムスタンプサーバ７の公開鍵Ｅｔを用いて復号することでダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２２）。

【００７７】

一方、ダイジェスト生成部６２は、ハッシュ関数ｆを用いてクライアント１から送られてきたコンテンツＣ１からダイジェストｆ（Ｓ１）を生成し（ステップ２２４）、付加情報から取り出したｆ（Ｓ２）及びｆ（Ｓ３）と結合して結合ダイジェストＦ（＝ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２４）。タイムスタンプ検証部６４は、結合ダイジェストＦからハッシュ関数Ｈを用いてダイジェストＨ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成し、これに受信した付加情報から取り出したタイムスタンプ生成時刻Ｔｔを付加してＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を得る。

【００７８】

以上のようにして比較対象のダイジェストが生成されると、２つのダイジェスト、すなわち、タイムスタンプの復号により得られたダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））と、コンテンツ管理サーバ４にて生成したダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））とを比較することで、コンテンツＣ１に付加されたタイムスタンプを検証する（ステップ２２５）。以上のようにして、簡易検証を行うことができる。

【００７９】

次に、通常検証の場合について説明するが、タイムスタンプ検証依頼側における処理は、簡易検証と同じなので説明を省略し、タイムスタンプ検証側の処理について説明する。

【００８０】

コンテンツ管理サーバ４において、クライアント１から発せられたタイムスタンプ生成依頼要求を受信すると（ステップ２２１）、タイムスタンプ検証部６４は、受信したコンテンツＣ１の付加情報に含まれているタイムスタンプＥｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を、タイムスタンプサーバ７の公開鍵Ｅｔを用いて復号することでダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２２）。ここまでの処理は、簡易検証と同じである。

【００８１】

一方、ダイジェスト生成部６２は、付加情報から取り出した他のコンテンツのＩＤ（＝ＩＤ２，ＩＤ３）をキーにして当該コンテンツＣ２，Ｃ３をコンテンツデータベース６８から読み出す。これにより、各コンテンツＣ１～Ｃ３を得ることができたので、ダイジェスト生成部６２は、ハッシュ関数ｆを用いて各コンテンツＣ１～Ｃ３からダイジェストｆ（Ｓ１），ｆ（Ｓ２），ｆ（Ｓ３）を生成し、そして結合ダイジェストＦ（＝ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２８）。

【００８２】

この後の処理は、簡易検証と同じであり、タイムスタンプ検証部６４は、結合ダイジェストＦからハッシュ関数Ｈを用いてダイジェストＨ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３

））を生成し、これに受信した付加情報から取り出したタイムスタンプ生成時刻Ｔｔを付加してＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を得る。

【００８３】

以上のようにして比較対象のダイジェストが生成されると、２つのダイジェスト、すなわち、タイムスタンプの復号により得られたダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））と、コンテンツ管理サーバ４にて生成したダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））とを比較することで、コンテンツＣ１に付加されたタイムスタンプを検証する（ステップ２２５）。以上のようにして、通常検証を行うことができる。

【００８４】

このように、通常検証の場合、コンテンツ管理サーバ４は、内部保有するコンテンツデータベース６８から他のコンテンツのＩＤをキーにコンテンツを取得し、そして他のコンテンツのダイジェストを自ら生成してダイジェストの比較を行えるようにした。このように、付加情報に含まれているダイジェストを用いないので、タイムスタンプ検証の確度を向上させることができる。

【００８５】

本実施の形態によれば、以上説明したように、複数のコンテンツに共通してタイムスタンプを取得した場合でもタイムスタンプ検証側において各コンテンツに付加されたタイムスタンプの検証を個々に行うことができる。これにより、タイムスタンプを利用する側は、コンテンツ個々にタイムスタンプを取得する必要がないので、コンテンツ毎にタイムスタンプを取得することによる煩わしさから解消される。一方、タイムスタンプ検証側では、タイムスタンプ検証の対象とするコンテンツ以外のコンテンツが送られてこなくても、タイムスタンプの検証を行うことができる。つまり、簡易検証の場合は、付加情報に含まれる他のコンテンツのダイジェストから、通常検証の場合は、付加情報に含まれる他のコンテンツのＩＤから、それぞれ共通してタイムスタンプが付加されたコンテンツの各ダイジェストを取得することができるので、タイムスタンプの検証に必要なダイジェストは、タイムスタンプ検証側で生成することができる。

【００８６】

実施の形態２．

本実施の形態におけるタイムスタンプ検証時のクライアント１における処理のフローチャートを図８に、タイムスタンプ検証時の通常検証の場合のコンテンツ管理サーバ４における処理のフローチャートを図９に、それぞれ示す。図８及び図９は、実施の形態１における図５及び図７に対応する図であるが、この図５，図７に示したフローチャートと比較すれば明らかなように、本実施の形態におけるクライアント１は、付加情報に含める他のコンテンツＩＤを暗号化してからコンテンツ管理サーバ４へ送ることを特徴としている。

【００８７】

以下、本実施の形態におけるタイムスタンプ検証時処理について説明する。ここでは、実施の形態１と同様に、コンテンツＩＤがそれぞれＩＤ１，ＩＤ２，ＩＤ３である３つのコンテンツＣ１，Ｃ２，Ｃ３に共通してタイムスタンプが生成され、このうちコンテンツＣ１に付加されたタイムスタンプの検証を行う場合を例にして説明する。また、各コンテンツＣ１～Ｃ３の署名対象領域をＳ１，Ｓ２，Ｓ３、署名情報領域をE１，Ｅ２，Ｅ３とする。なお、図８，９において、図５，７と同じ処理ステップには同じ符号を付け説明を適宜省略する。また、他のコンテンツに関する情報としてコンテンツＩＤを使用しない簡易検証については、実施の形態１と同じ処理になるので説明を省略する。また、本実施の形態におけるシステム構成も実施の形態１と同じなので説明を省略する。

【００８８】

クライアント１において、付加情報生成部２６に含まれる他コンテンツ情報生成部３２は、ハッシュ関数ｆを用いて他のコンテンツＣ２，Ｃ３のダイジェストｆ（Ｓ２），ｆ（Ｓ３）をそれぞれ生成する。また、他のコンテンツに関する情報として、更に他のコンテンツＣ２，Ｃ３の識別情報｛ＩＤ２，ＩＤ３｝も集約するが、このとき、他のコンテンツ

のＩＤを、タイムスタンプ検証を行うコンテンツ管理サーバ４の公開鍵Ｅｓで暗号化した後に付加情報に含める（ステップ１２１，１２２）。このようにして生成された各付加情報は、次のようになる。

Ｅ１＝（Ｅｎｃ（Ｅｓ，ＩＤ２＋ＩＤ３），｛ｆ（Ｓ２），ｆ（Ｓ３）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

【００８９】

なお、参考までにコンテンツＣ２，Ｃ３の付加情報は、次のようになる。

Ｅ２＝（Ｅｎｃ（Ｅｓ，ＩＤ３＋ＩＤ１），｛ｆ（Ｓ３），ｆ（Ｓ１）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

Ｅ３＝（Ｅｎｃ（Ｅｓ，ＩＤ１＋ＩＤ２），｛ｆ（Ｓ１），ｆ（Ｓ２）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

【００９０】

このようにして生成された付加情報Ｅ１は、コンテンツＣ１を格納する領域Ｓ１に付加されてタイムスタンプ生成依頼要求としてコンテンツ管理サーバ４へ送信される（ステップ１１６）。

【００９１】

コンテンツ管理サーバ４において、クライアント１から発せられたタイムスタンプ生成依頼要求を受信すると（ステップ２２１）、タイムスタンプ検証部６４は、受信したコンテンツＣ１の付加情報に含まれているタイムスタンプＥｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を復号してダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２２）。

【００９２】

一方、ダイジェスト生成部６２は、コンテンツＣ１の付加情報から他のコンテンツのＩＤ、すなわちＩＤ２，ＩＤ３を取り出すが、本実施の形態においては、他のコンテンツＩＤは、自己の公開鍵で暗号化されているので、ダイジェスト生成部６２は、この公開鍵に対応した自己の秘密鍵で復号することでコンテンツＩＤを抽出する（ステップ２２９）。この抽出したコンテンツＩＤを次のように表すことができる。

ＩＤｘ＝Ｄｅｃ（Ｄｓ，Ｅｎｃ（Ｅｓ，ＩＤ２＋ＩＤ３））　（ｘ＝２，３）

【００９３】

このように、復号により他のコンテンツのＩＤを取得した後の処理は、実施の形態１と同じである。すなわち、ダイジェスト生成部６２は、復号により得た他のコンテンツのＩＤ（＝ＩＤ２，ＩＤ３）をキーにして当該コンテンツＣ２，Ｃ３をコンテンツデータベース６８から読み出すと、受信したコンテンツＣ１と共にそれぞれのダイジェストｆ（Ｓ１），ｆ（Ｓ２），ｆ（Ｓ３）を生成し（ステップ２２７）、そして結合ダイジェストＦ（＝ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２８）。続いて、タイムスタンプ検証部６４は、結合ダイジェストＦからハッシュ関数Ｈを用いてダイジェストＨ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成し、これに受信した付加情報から取り出したタイムスタンプ生成時刻Ｔｔを付加してＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を得る。

【００９４】

以上のようにして比較対象のダイジェストが生成されると、タイムスタンプ検証部６４は、タイムスタンプの復号により得られたダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））と、コンテンツ管理サーバ４にて生成したダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））とを比較することで、コンテンツＣ１に付加されたタイムスタンプを検証する（ステップ２２５）。以上のようにして、通常検証を行うことができる。

【００９５】

本実施の形態によれば、コンテンツＩＤを暗号化してからクライアント１からコンテンツ管理サーバ４へ送るようにしたので、コンテンツＩＤの改竄防止を図ることによりタイムスタンプ検証の確度を向上させることができる。

【００９６】
実施の形態３．
図１０は、本実施の形態におけるタイムスタンプ検証システムのブロック構成図である。図１０において、図２と同じ構成には、同じ符号を付け、説明を省略する。本実施の形態においては、コンテンツ管理サーバ４に乱数生成部７２及び乱数保持部７４を追加した構成を有している。乱数生成部７２は、乱数を生成する手段である。乱数生成部７２が生成した乱数は、乱数の生成時間情報と共にコンテンツに付加されてクライアント１へダウンロードされるが、コンテンツがダウンロードされたとき、そのダウンロードされたコンテンツのＩＤ及び乱数生成時間情報と組にして乱数保持部７４に登録される。この乱数保持部７４に登録されるデータ構成例を図１１に示す。なお、乱数生成部７２が有する処理機能は、当該処理機能を発揮するタイムスタンプ検証プログラムと、コンテンツ管理サーバ４を構成するハードウェアとの協調動作により実現される。
【００９７】
次に、本実施の形態におけるタイムスタンプの生成処理及び検証処理について具体例を用いて説明する。ここでは、実施の形態１，２と同様に、コンテンツＩＤがそれぞれＩＤ１，ＩＤ２，ＩＤ３である３つのコンテンツＣ１，Ｃ２，Ｃ３に共通してタイムスタンプが生成され、このうちコンテンツＣ１に付加されたタイムスタンプの検証を行う場合を例にして説明する。また、各コンテンツＣ１～Ｃ３の署名対象領域をＳ１，Ｓ２，Ｓ３、署名情報領域をE１，Ｅ２，Ｅ３とする。なお、本実施の形態の説明に用いる各フローチャートにおいて、上記各実施の形態のフローチャートに含まれる同じ処理ステップには同じ符号を付け説明を適宜省略する。以降の説明で明らかになるように、本実施の形態は、実施の形態２が付加情報に含める他のコンテンツＩＤのみを暗号化するのに対し、本実施の形態では、他のコンテンツＩＤに乱数及び乱数生成時間情報を付加してから暗号化することを特徴としている。まず、本実施の形態におけるタイムスタンプ生成時における処理を、図１２及び図１３に示した各フローチャートを用いて説明する。
【００９８】
コンテンツ管理サーバ４において、クライアント１からコンテンツのダウンロード要求が送られてくると、乱数生成部７２は、要求されたコンテンツ毎に乱数を生成する（ステップ２３１）。そして、コンテンツ配信部４２は、要求された署名対象のコンテンツＣ１～Ｃ３をコンテンツデータベース６８から取り出し、そのコンテンツＣ１～Ｃ３に乱数ｒ１～ｒ３及び各乱数生成時間情報Ｔ１を付加して当該クライアント１へ送信する（ステップ２３２）。なお、各乱数の生成時刻は各コンテンツとも同じＴ１とする。そして、コンテンツ配信部４２は、図１１に例示したように、送信したコンテンツＣ１～Ｃ３の各ＩＤと乱数と乱数生成時間情報とを組にして乱数保持部７４に登録する（ステップ２３３）。
【００９９】
クライアント１において、コンテンツＣ１～Ｃ３及び乱数をコンテンツ管理サーバ４から取得すると（ステップ１３１）、ダイジェスト生成部２０は、ハッシュ関数ｆを用いてダイジェストｆ（Ｓ１），ｆ（Ｓ２），ｆ（Ｓ３）をそれぞれ生成し（ステップ１１２）、コンテンツ管理サーバ４へ送信することでタイムスタンプの生成依頼要求を出す（ステップ１１３）。
【０１００】
コンテンツ管理サーバ４は、クライアント１からのタイムスタンプの生成依頼要求を受信すると（ステップ２１２）、タイムスタンプ要求部５０は、生成依頼要求に含まれている複数のダイジェストＦ（＝ｆ（Ｓ１＋Ｓ２＋Ｓ３）を結合し、ハッシュ関数Ｈを用いてダイジェストＨ（Ｆ）生成し（ステップ２１３）、タイムスタンプサーバ７へ送信する（ステップ２１４）。そして、タイムスタンプサーバ７から送られてきたタイムスタンプトークンを受信すると、タイムスタンプ情報、すなわちＴｔとＨ（Ｆ）をクライアント１へ通知する（ステップ２１７）。
【０１０１】
このようにして、クライアント１は、コンテンツＣ１～Ｃ３に共通したタイムスタンプ

を得ることができるが、タイムスタンプ生成依頼処理部１４は、コンテンツ毎に、コンテンツＩＤ，乱数生成時間情報、乱数及びタイムスタンプ情報を対応付けしてタイムスタンプ保持テーブル３６に保存する（ステップ１３３）。このタイムスタンプ保持テーブル３６に設定登録されたデータ構成例を図１４に示す。

【０１０２】

続いて、タイムスタンプ検証時における処理のうち通常検証について図１５及び図１６に示した各フローチャートを用いて説明する。なお、付加情報に含まれるコンテンツＩＤを使用しない簡易検証については、実施の形態２と同じなので説明を省略する。ここでもコンテンツＣ１に付加されたタイムスタンプの検証を行う場合を例にして説明する。

【０１０３】

クライアント１において、付加情報生成部２６に含まれる他コンテンツ情報生成部３２は、ハッシュ関数ｆを用いて他のコンテンツＣ２，Ｃ３のダイジェストｆ（Ｓ２），ｆ（Ｓ３）をそれぞれ生成する。また、他のコンテンツに関する情報として、更に他のコンテンツＣ２，Ｃ３の識別情報｛ＩＤ２，ＩＤ３｝も集約するが、このとき、他コンテンツ情報生成部３２は、コンテンツ取得時にコンテンツＣ２，Ｃ３と共にした乱数ｒ２，ｒ３及び乱数時間情報Ｔ１をタイムスタンプ保持テーブル３６から読み出し、他のコンテンツのＩＤに、その乱数を結合してからコンテンツ管理サーバ４の公開鍵Ｅｓで暗号化し（ステップ１３４）、また、乱数時間情報Ｔ１をコンテンツ管理サーバ４の公開鍵Ｅｓで暗号化し、そしてコンテンツＣ１の付加情報にそれぞれ含める（ステップ１２２）。以上の処理にて生成された各付加情報は、次のようになる。

Ｅ１＝（Ｅｎｃ（Ｅｓ，ｒ１＋ＩＤ２＋ＩＤ３），Ｅｎｃ（Ｅｓ，Ｔ１），｛ｆ（Ｓ２），ｆ（Ｓ３）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

【０１０４】

なお、参考までにコンテンツＣ２，Ｃ３の付加情報は、次のようになる。

Ｅ２＝（Ｅｎｃ（Ｅｓ，ｒ２＋ＩＤ３＋ＩＤ１），Ｅｎｃ（Ｅｓ，Ｔ１），｛ｆ（Ｓ３），ｆ（Ｓ１）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

Ｅ３＝（Ｅｎｃ（Ｅｓ，ｒ３＋ＩＤ１＋ＩＤ２），Ｅｎｃ（Ｅｓ，Ｔ１），｛ｆ（Ｓ１），ｆ（Ｓ２）｝，Ｔｔ，Ｅｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））｝

【０１０５】

このようにして生成された付加情報Ｅ１は、コンテンツＣ１を格納する領域Ｓ１に付加されてタイムスタンプ生成依頼要求としてコンテンツ管理サーバ４へ送信される（ステップ１１６）。

【０１０６】

コンテンツ管理サーバ４において、クライアント１から発せられたタイムスタンプ生成依頼要求を受信すると（ステップ２２１）、タイムスタンプ検証処理部４６は、受信したコンテンツＣ１の付加情報に含まれているタイムスタンプＥｎｃ（Ｄｔ，Ｔｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を復号してダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２２）。

【０１０７】

一方、ダイジェスト生成部６２は、コンテンツＣ１の付加情報から他のコンテンツのＩＤ、すなわちＩＤ２，ＩＤ３を取り出すが、本実施の形態においては、他のコンテンツＩＤは、自己の公開鍵で暗号化されているので、ダイジェスト生成部６２は、この公開鍵に対応した自己の秘密鍵で復号することでコンテンツＩＤを抽出する（ステップ２３４）。但し、本実施の形態では、コンテンツＩＤと共に乱数ｒ１及び乱数生成時間情報Ｔ１が復号対象となっている。この復号の内容は、次のように表すことができる。

ＩＤｘ，ｒ１＝Ｄｅｃ（Ｄｓ，Ｅｎｃ（Ｅｓ，ｒ１＋ＩＤ２＋ＩＤ３））

但し、ｘ＝２，３

Ｔ１＝Ｄｅｃ（Ｄｓ，Ｅｎｃ（Ｔ１））

【０１０８】

上記式で示されているように、復号された他のコンテンツＣ２，Ｃ３のＩＤ（ＩＤ２，ＩＤ３）には、乱数ｒ１が結合されているので、タイムスタンプ検証処理部４６は、検証対象のコンテンツＣ１のコンテンツＩＤ（＝ＩＤ１）及び復号された乱数発生時間情報Ｔ１の組をキーにして乱数保持部７４を検索し、乱数ｒ１を取り出す（ステップ２３５）。コンテンツＣ１は、１乃至複数のクライアント１によって複数回ダウンロードされている可能性もあるので、本実施の形態では、コンテンツＩＤと乱数発生時間情報との組で乱数を一意に特定できるようにした。そして、その取り出した乱数ｒ１を、復号した結果（ＩＤｘ，ｒ１）から差し引くことでＩＤｘ（ｘ＝２，３）を抽出する。その後の処理は、実施の形態２と同じである。すなわち、ダイジェスト生成部６２は、コンテンツ読出部６０に指示をすることでコンテンツＣ２，Ｃ３を取り出し、ハッシュ関数ｆを用いて各コンテンツのダイジェストｆ（Ｓ１），ｆ（Ｓ２），ｆ（Ｓ３）を生成し（ステップ２２７）、これらを結合して結合ダイジェストＦ（＝ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成する（ステップ２２８）。続いて、タイムスタンプ検証部６４は、結合ダイジェストＦからハッシュ関数Ｈを用いてダイジェストＨ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を生成し、これに受信した付加情報から取り出したタイムスタンプ生成時刻Ｔｔを付加してＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））を得る。

【０１０９】

以上のようにして比較対象のダイジェストが生成されると、タイムスタンプ検証部６４は、タイムスタンプの復号により得られたダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））と、コンテンツ管理サーバ４にて生成したダイジェストＴｔ＋Ｈ（ｆ（Ｓ１）＋ｆ（Ｓ２）＋ｆ（Ｓ３））とを比較することで、コンテンツＣ１に付加されたタイムスタンプを検証する（ステップ２２５）。以上のようにして、通常検証を行うことができる。

【０１１０】

本実施の形態によれば、コンテンツＩＤを暗号化してからクライアント１からコンテンツ管理サーバ４へ送るようにしたので、実施の形態２と同様にコンテンツＩＤの改竄防止を図ることでタイムスタンプ検証の確度を向上させることができる。更に、暗号化する際にコンテンツＩＤに乱数を結合することで、次のような効果を奏することができる。ここでもコンテンツＣ１に付加されたタイムスタンプの検証を行う場合を例にして説明する。

【０１１１】

例えば、不正アクセス者による不正行為によってタイムスタンプ情報領域Ｅ１に格納された付加情報のうちコンテンツＩＤ（＝ＩＤ２，ＩＤ３）を異なるコンテンツＩＤ、例えば、ＩＤ１，ＩＤ２に書き換えるという改竄がされたとする。このような改竄は、例えばコンテンツＣ３の付加情報でコンテンツＣ１の付加情報を上書きすれば可能になる。乱数をコンテンツＩＤに結合していない場合、コンテンツ管理サーバ４は、コンテンツＣ１の付加情報から改竄されたコンテンツＩＤ、すなわちＩＤ１，ＩＤ２を取得でき、そしてコンテンツデータベース６８からコンテンツＣ１，Ｃ２を正常に取得することができる。このように、コンテンツが正常に取得できた後にダイジェストの比較処理を行うが、タイムスタンプの復号により生成されたダイジェストと比較するダイジェストは、本来コンテンツＣ１，Ｃ２，Ｃ３から生成される結合ダイジェストであるべきところを、改竄によりコンテンツＣ１，Ｃ２，Ｃ１から生成されているので、各ダイジェストは完全に一致しない。つまり、タイムスタンプの検証は失敗する。この場合、コンテンツ管理サーバ４は、付加情報からコンテンツＩＤ（＝ＩＤ１，ＩＤ２）が正常に抽出でき、かつコンテンツＣ１，Ｃ２をコンテンツデータベース６８から正常に取り出すことができたので、検証の失敗の原因は、署名対象領域Ｓ１に格納されたコンテンツＣ１が改竄されたと誤って認識してしまう。

【０１１２】

これに対し、乱数をコンテンツＩＤに結合させた場合、コンテンツ管理サーバ４は、前

述したようにコンテンツＣ１を上書きしたコンテンツＣ３の乱数、すなわち乱数ｒ１ではなく乱数ｒ３を取り出すことになる。この結果、前述した式、
ＩＤｘ，ｒ１＝Ｄｅｃ（Ｄｓ，Ｅｎｃ（Ｅｓ，ｒ１＋ＩＤ２＋ＩＤ３））
但し、ｘ＝２，３
で取り出したＩＤｘ，ｒ１（ｘ＝２，３）から乱数ｒ３を差し引いても、ＩＤ２とＩＤ３を正しく抽出することができない。このため、コンテンツ管理サーバ４は、コンテンツデータベース６８からコンテンツを正常に取り出すことができないので、署名対象領域Ｓ１に格納されたコンテンツデータではなく署名情報領域Ｅ１に格納された付加情報が改竄されたと正しく認識することができる。

【０１１３】

なお、本実施の形態において、コンテンツＩＤと共に乱数生成時間情報を対応付けして乱数保持部７４に登録したのは、コンテンツに付加した乱数を一意に特定できるようにするためである。従って、一意に特定できる情報であれば、乱数生成時間情報に限定する必要はない。例えば、コンテンツの送信時間情報でもよいし、ダウンロードというイベントの識別情報であってもよい。

【図面の簡単な説明】

【０１１４】

【図１】本発明に係るタイムスタンプ検証システムの一実施の形態を示した全体構成図である。

【図２】実施の形態１におけるタイムスタンプ検証システムのブロック構成図である。

【図３】実施の形態１においてタイムスタンプを生成する際のクライアント側における処理を示したフローチャートである。

【図４】実施の形態１においてタイムスタンプを生成する際のコンテンツ管理サーバ側における処理を示したフローチャートである。

【図５】実施の形態１においてタイムスタンプの検証を依頼するクライアント側における処理を示したフローチャートである。

【図６】実施の形態１において簡易検証におけるタイムスタンプの検証を行うクライアント側における処理を示したフローチャートである。

【図７】実施の形態１において通常検証におけるタイムスタンプの検証を行うクライアント側における処理を示したフローチャートである。

【図８】実施の形態２においてタイムスタンプの検証を依頼するクライアント側における処理を示したフローチャートである。

【図９】実施の形態２において通常検証におけるタイムスタンプの検証を行うクライアント側における処理を示したフローチャートである。

【図１０】実施の形態３におけるタイムスタンプ検証システムのブロック構成図である。

【図１１】実施の形態３における乱数保持部に登録されるデータ構成例を示した図である。

【図１２】実施の形態３においてタイムスタンプを生成する際のコンテンツ管理サーバ側における処理を示したフローチャートである。

【図１３】実施の形態３においてタイムスタンプを生成する際のコンテンツ管理サーバ側における処理を示したフローチャートである。

【図１４】実施の形態３におけるタイムスタンプ保持テーブルに設定登録されるデータ構成例を示した図である。

【図１５】実施の形態３においてタイムスタンプの検証を依頼するクライアント側における処理を示したフローチャートである。

【図１６】実施の形態３において通常検証におけるタイムスタンプの検証を行うクライアント側における処理を示したフローチャートである。

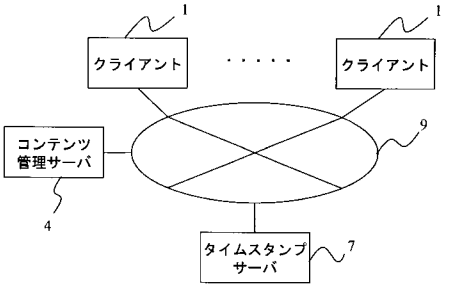
【符号の説明】

【０１１５】

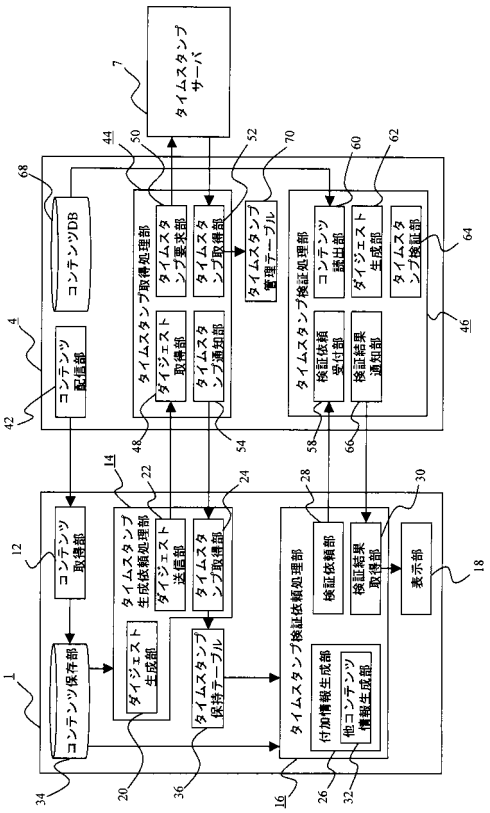
１　クライアント、４　コンテンツ管理サーバ、７　タイムスタンプサーバ、９　公衆

網、１２　コンテンツ取得部、１４　タイムスタンプ生成依頼処理部、１６　タイムスタンプ検証依頼処理部、１８　表示部、２０　ダイジェスト生成部、２２　ダイジェスト送信部、２４　タイムスタンプ取得部、２６　付加情報生成部、２８　検証依頼部、３０　検証結果取得部、３２　他コンテンツ情報生成部、３４　コンテンツ保存部、３６　タイムスタンプ保持テーブル、４２　コンテンツ配信部、４４　タイムスタンプ取得処理部、４６　タイムスタンプ検証処理部、４８　ダイジェスト取得部、５０　タイムスタンプ要求部、５２　タイムスタンプ取得部、５４　タイムスタンプ通知部、５８　検証依頼受付部、６０　コンテンツ読出部、６２　ダイジェスト生成部、６４　タイムスタンプ検証部、６６　検証結果通知部、６８　コンテンツデータベース、７０　タイムスタンプ管理テーブル、７２　乱数生成部、７４　乱数保持部。

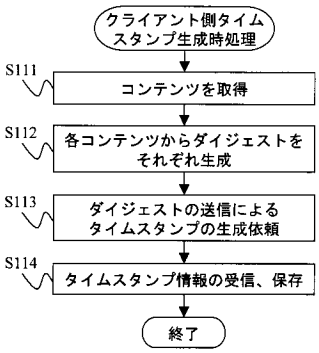
【図１】



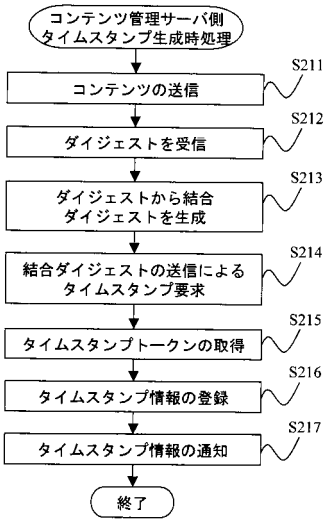
【図２】



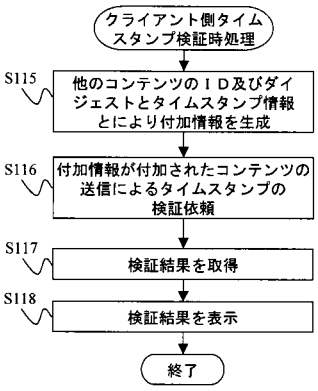
【図３】


クライアント側タイムスタンプ生成時処理
S111
コンテンツを取得
S112
各コンテンツからダイジェストをそれぞれ生成
S113
ダイジェストの送信によるタイムスタンプの生成依頼
S114
タイムスタンプ情報の受信、保存
終了

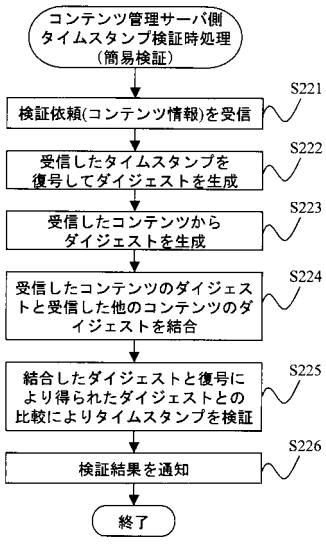
【図４】


コンテンツ管理サーバ側タイムスタンプ生成時処理
S211
コンテンツの送信
S212
ダイジェストを受信
S213
ダイジェストから結合ダイジェストを生成
S214
結合ダイジェストの送信によるタイムスタンプ要求
S215
タイムスタンプトークンの取得
S216
タイムスタンプ情報の登録
S217
タイムスタンプ情報の通知
終了

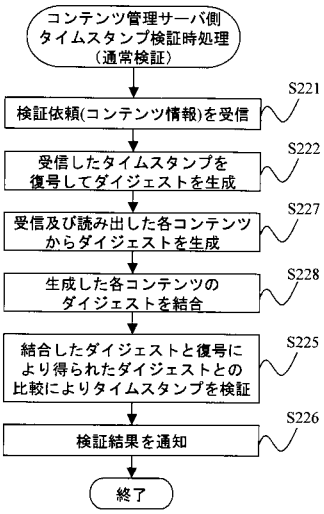
【図５】


クライアント側タイムスタンプ検証時処理
S115
他のコンテンツのＩＤ及びダイジェストとタイムスタンプ情報とにより付加情報を生成
S116
付加情報が付加されたコンテンツの送信によるタイムスタンプの検証依頼
S117
検証結果を取得
S118
検証結果を表示
終了

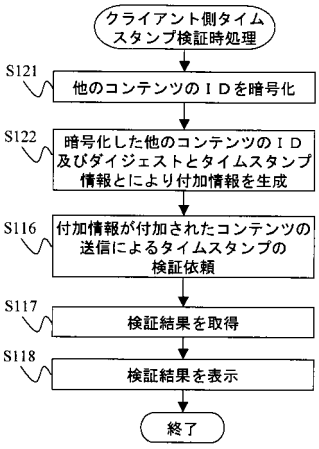
【図６】


コンテンツ管理サーバ側タイムスタンプ検証時処理（簡易検証）
S221
検証依頼(コンテンツ情報)を受信
S222
受信したタイムスタンプを復号してダイジェストを生成
S223
受信したコンテンツからダイジェストを生成
S224
受信したコンテンツのダイジェストと受信した他のコンテンツのダイジェストを結合
S225
結合したダイジェストと復号により得られたダイジェストとの比較によりタイムスタンプを検証
S226
検証結果を通知
終了

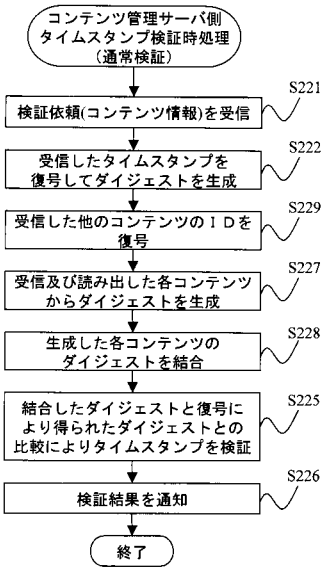
【図７】


コンテンツ管理サーバ側
タイムスタンプ検証時処理
（通常検証）
検証依頼(コンテンツ情報)を受信
S221
受信したタイムスタンプを
復号してダイジェストを生成
S222
受信及び読み出した各コンテンツ
からダイジェストを生成
S227
生成した各コンテンツの
ダイジェストを結合
S228
結合したダイジェストと復号に
より得られたダイジェストとの
比較によりタイムスタンプを検証
S225
検証結果を通知
S226
終了

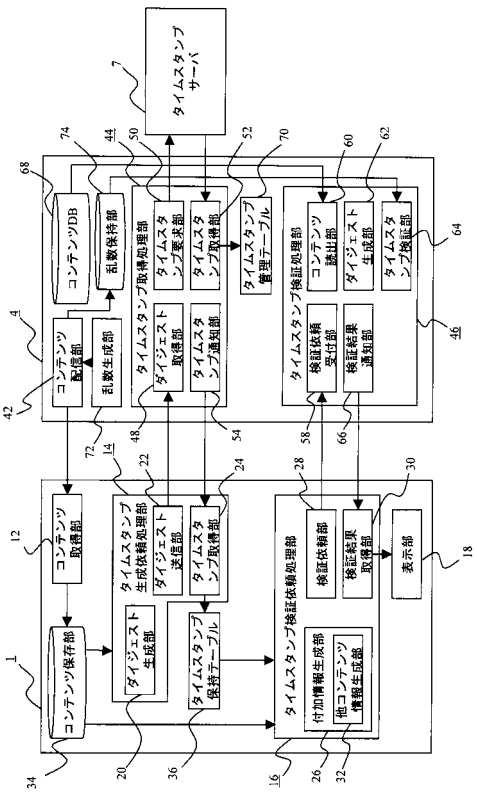
【図８】


クライアント側タイム
スタンプ検証時処理
S121
他のコンテンツのＩＤを暗号化
S122
暗号化した他のコンテンツのＩＤ
及びダイジェストとタイムスタンプ
情報とにより付加情報を生成
S116
付加情報が付加されたコンテンツの
送信によるタイムスタンプの
検証依頼
S117
検証結果を取得
S118
検証結果を表示
終了

【図９】


コンテンツ管理サーバ側
タイムスタンプ検証時処理
（通常検証）
検証依頼(コンテンツ情報)を受信
S221
受信したタイムスタンプを
復号してダイジェストを生成
S222
受信した他のコンテンツのＩＤを
復号
S229
受信及び読み出した各コンテンツ
からダイジェストを生成
S227
生成した各コンテンツの
ダイジェストを結合
S228
結合したダイジェストと復号に
より得られたダイジェストとの
比較によりタイムスタンプを検証
S225
検証結果を通知
S226
終了

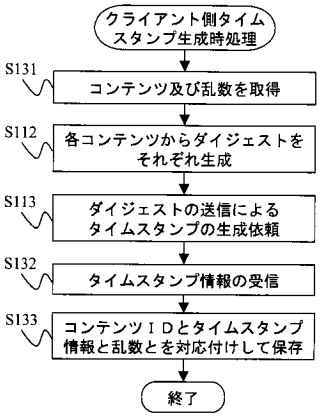
【図１０】


タイムスタンプ
サーバ
7
コンテンツDB
乱数保持部
タイムスタンプ取得処理部
タイムスタンプ要求部
タイムスタンプ取得部
タイムスタンプ管理テーブル
タイムスタンプ検証処理部
コンテンツ読出部
ダイジェスト生成部
タイムスタンプ検証部
コンテンツ配信部
乱数生成部
ダイジェスト取得部
タイムスタンプ通知部
検証依頼受付部
検証結果通知部
コンテンツ取得部
タイムスタンプ生成依頼処理部
ダイジェスト送信部
タイムスタンプ取得部
検証依頼部
検証結果取得部
表示部
コンテンツ保存部
ダイジェスト生成部
タイムスタンプ保持テーブル
タイムスタンプ検証依頼処理部
付加情報生成部
他コンテンツ情報生成部

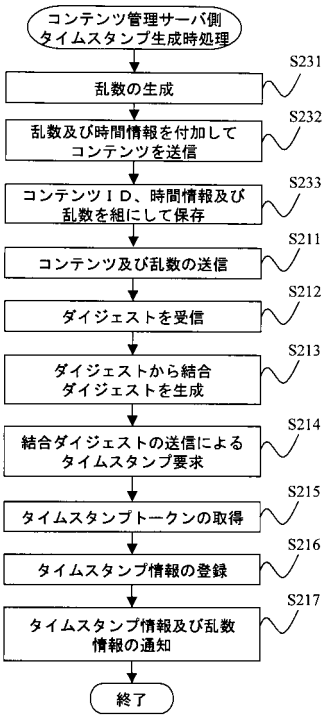
【図１１】

コンテンツＩＤ	乱数生成時間情報	乱数
ＩＤ１	Ｔ１	ｒ１
ＩＤ２	Ｔ１	ｒ２
ＩＤ３	Ｔ１	ｒ３
ＩＤ１	Ｔ２	ｒ４

【図１２】



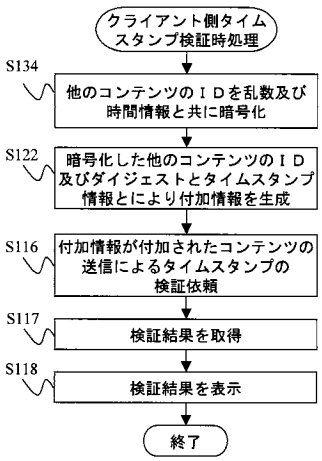
【図１３】



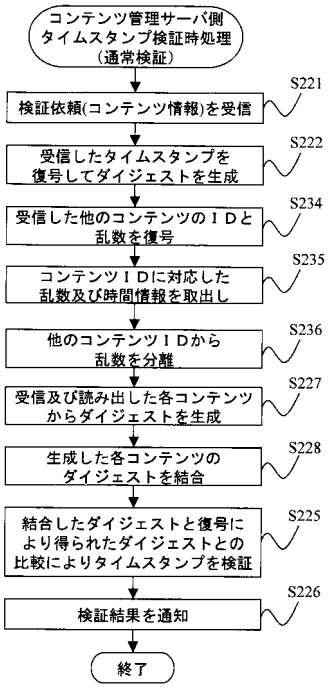
【図１４】

コンテンツＩＤ	乱数生成時間情報	乱数	タイムスタンプ情報
ＩＤ１	Ｔ１	ｒ１	Tt, TSValue
ＩＤ２	Ｔ１	ｒ２	Tt, TSValue
ＩＤ３	Ｔ１	ｒ３	Tt, TSValue

【図１５】



【図１６】



フロントページの続き

(56)参考文献 特開２００５－０５１７３４（ＪＰ，Ａ）
特開２００４－０２３６４９（ＪＰ，Ａ）
特開平１０－３２６０７８（ＪＰ，Ａ）
特開平１０－１０５０５７（ＪＰ，Ａ）
特開２００１－１４２３９８（ＪＰ，Ａ）
特開２０００－２８６８３６（ＪＰ，Ａ）
特開２００５－０２７０５９（ＪＰ，Ａ）
特開２００３－３３８８１５（ＪＰ，Ａ）
特開２００４－３２０３９８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２