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

特許第4266096号
(P4266096)

(45)発行日　平成21年5月20日(2009.5.20)　(24)登録日　平成21年2月27日(2009.2.27)

(51)Int.Cl.		F I		
G06F 12/00	(2006.01)	G06F	12/00	537Z
G06F 21/24	(2006.01)	G06F	12/14	560C
G06F 12/14	(2006.01)	G06F	12/14	ZEC

請求項の数 4　(全 17 頁)

(21)出願番号　特願2002-85836(P2002-85836)
(22)出願日　平成14年3月26日(2002.3.26)
(65)公開番号　特開2003-280972(P2003-280972A)
(43)公開日　平成15年10月3日(2003.10.3)
審査請求日　平成17年2月22日(2005.2.22)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)復代理人　100102587
弁理士　渡邊　昌幸
(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　伊藤　信治
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】ファイル保管システムとＮＡＳサーバ

(57)【特許請求の範囲】
【請求項１】
利用者用計算機と、１以上の利用者用計算機とネットワークを介して接続され当該利用者用計算機から受信したファイルの保管を行うストレージサーバとからなるファイル保管システムであって、
１以上のストレージサーバとネットワークを介して接続され、各ストレージサーバで保管しているファイルの正当性を保証するためのデータを集約して保証手続きを代行する集約サーバを設け、
前記ストレージサーバは、
上記ファイルを、当該ファイルが作成および更新される毎に、該それぞれの時刻でのファイルを連鎖させるための連鎖用情報を付与して第１の連鎖データとして保管すると共に、更新されたファイルの保管時には、当該ファイルに対応する前回保管した第１の連鎖データを用いて連鎖用情報を生成し、該生成した連鎖用情報を当該更新されたファイルに付与して当該更新されたファイルに対応する第１の連鎖データとして保管する手段と、
上記利用者用計算機からのファイルの現在の状態を証明可能に保つ要求（ファイル状態固定要求）に応じて、当該ファイルに対応する第１の連鎖データに秘密鍵で署名して当該ファイルの保証要求データを生成し、生成した保証要求データを上記集約サーバに送出する手段と、
上記集約サーバが上記保証要求データを用いて生成したファイル固定保証データを当該集約サーバから受信して保管する手段と

を有し、
上記集約サーバは、
各ストレージサーバから受信した保証要求データをヒステリシス署名して当該ファイルの第２の連鎖データを生成して保管する手段と、
予め定められたタイミングで、前回のタイミングから今回のタイミングまでに生成して保管した当該ファイルの各第２の連鎖データからなるファイル固定保証データを生成し、生成したファイル固定保証データを、当該ファイル固定保証データの生成に用いた保証要求データを送出してきたストレージサーバに送出する手段とを有する
ことを特徴とするファイル保管システム。
【請求項２】
請求項１に記載のファイル保管システムであって、
１以上の上記集約サーバにネットワークを介して接続された公開サーバを設け、
上記集約サーバは、上記予め定められたタイミングで、該タイミングまでに生成して保管した当該ファイルの最新の第２の連鎖データを、正当性保証データとして上記公開サーバに送信する手段を有し、
上記公開サーバは、１以上の上記集約サーバから受信した上記正当性保証データを公表する手段を有し、
上記集約サーバが保管するファイル固定保証データは、上記公開サーバが公表した上記正当性保証データを含むことを特徴とするファイル保管システム。
【請求項３】
請求項１もしくは請求項２のいずれかに記載のファイル保管システムであって、
上記ストレージサーバにおける上記保証要求データを生成する手段は、
上記利用者計算機から送られてくる、当該ファイルのファイル名、作成者名、アクセス許可情報、アクセス時刻の、少なくともいずれか１つを含むファイル付随情報を用いて上記保証要求データを生成する
ことを特徴とするファイル保管システム。
【請求項４】
１以上の利用者用計算機とネットワークを介して接続され、当該利用者用計算機ファイルの保管を行うＮＡＳサーバであって、請求項１から請求項３のいずれかに記載のファイル保管システムにおけるストレージサーバの各手段を具備したことを特徴とするＮＡＳサーバ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ディジタルデータ、ファイルの保管技術に係わり、特に、ＮＡＳ(Network Attached Storage)等、ネットワークを介してファイルを安全に保管するのに好適なファイル保管技術に関するものである。
【０００２】
【従来の技術】
ネットワークを利用してファイルを保管する技術には、例えば、ＮＡＳがある。このＮＡＳは、ＬＡＮ（Local Area Network）等のネットワークに直接接続されるストレージ（外部記憶装置）で、ストレージ・マネージメントソフトウエア、ＮＡＳオペレーティング・システム、グラフィカル・ユーザー・インタフェースと各種ハードウエア(プロセッサ、メモリ、ストレージインタフェース、ネットワークインタフェースなど)により構成される。
【０００３】
これらの要素技術により、ＮＡＳ装置（ＮＡＳサーバ）は、ネットワーク上でファイルを共有するための独立したファイルサーバとして機能し、クライアントからは、従来のファイルサーバへアクセスしているのと同様なオペレーションが可能となる。
【０００４】

しかし、従来のＮＡＳサーバは、格納したデータの存在時刻や非改ざん性を長期にわたって証明可能とする機能は有していない。そのため、データの存在時刻や非改ざん性を長期にわたって証明可能としたい場合は、ＮＡＳ利用者が、ＮＡＳにデータを保存する前に、予め何らかの保証措置を講ずる必要がある。

【０００５】

このような保証措置を講ずるためには、特別な装置を必要とするなど、コストがかかり、一般のＮＡＳ利用者にとっては負担が大きい。

【０００６】

【発明が解決しようとする課題】

解決しようとする問題点は、従来の技術では、利用者に負担をかけずに、ストレージサーバにおいて保管しているディジタルデータの存在時刻や非改ざん性を長期にわたって証明可能とすることができない点である。

【０００７】

本発明の目的は、これら従来技術の課題を解決し、ＮＡＳ等、ネットワークを利用してディジタルデータの保管を行うストレージシステムの信頼性および利便性の向上を図ることを可能とすることである。

【０００８】

【課題を解決するための手段】

上記目的を達成するため、本発明では、ＮＡＳサーバ（１０３）等において、格納するデータの存在時刻や非改ざん性を長期にわたって証明し、データの保証を可能とする。例えば、ＮＡＳサーバ（１０３）は、ＮＡＳ利用者からの要求を受けて、保証対象ファイルに対する保証データ（長期経過後にも保証要求時点から改竄されていないことを証明することができる証拠情報）を生成し、保証対象ファイルと共に保存する。このように、保証データの生成処理を、ファイルを保存するＮＡＳサーバ（１０３）側で行うので、ＮＡＳ利用者にとっては負担が軽減される。また、ＮＡＳサーバ（１０３）にとっては、保証対象ファイルとそれに対する保証データが一体として管理できるので管理が容易となる。

【０００９】

また、ＮＡＳサーバ（１０３）において生成される保証データは、公開サーバ（１０５）によって新聞公表等がなされたデータを含む。これにより、保証データの改竄は著しく困難になる。また、この困難性は、実社会との対応（例：新聞紙面に掲載された情報）によって達成されているため、たとえ、保証要求時点から長期経過後に、暗号ブレイク（暗号技術で利用される秘密情報の漏洩や、暗号解読技術の進歩など、何らかの原因によって暗号技術が危殆化すること）がおこったとしても尚、保証データの信頼性を確保することができる。

【００１０】

また、保証データ生成のために、ＮＡＳサーバ（１０３）が公開サーバ（１０５）を利用するときに、途中に集約サーバ（１０４）を設け、集約サーバ（１０４）が、多数のＮＡＳサーバ（１０３）からの要求をまとめてデータサイズを削減し、公開サーバ（１０５）に送るようにする。これにより、公開サーバ（１０５）にとっては、処理の削減が可能となり、ＮＡＳサーバ（１０３）にとっては、直接公開サーバ（１０５）によって公開してもらう必要がなくなるため、コストが削減できる。さらに、集約サーバ（１０４）を設け、複数のＮＡＳサーバ（１０３）からの要求を集約することにより、複数のＮＡＳサーバ（１０３）における各処理間の相対的な時間的順序関係が証明可能となる。

【００１１】

【発明の実施の形態】

以下、本発明の実施の形態を、図面により詳細に説明する。

【００１２】

図１は、本発明に係わるディジタルデータ保管システムの構成例を示すブロック図であり、図２は、図１におけるＮＡＳサーバ１０３で生成される連鎖データの構成例を示す説明図、図３は、図１におけるＮＡＳサーバ１０３から集約サーバ１０４に送信される保証要

求データの構成例を示す説明図、図４は、図１におけるＮＡＳサーバ１０３で保持するファイル固定保証データの構成例を示す説明図、図５は、図１におけるディジタルデータ保管システムの概略構成例を示すブロック図、図６は、図１におけるＮＡＳサーバ１０３の構成例を示すブロック図である。

【００１３】

図１および図５に示すシステムでは、ＮＡＳサーバ１０３の利用者用ＰＣ１０２（ＰＣ：パーソナルコンピュータ）と、ＮＡＳサーバ１０３利用者のファイルを保管するＮＡＳサーバ１０３と、ＮＡＳサーバ１０３が保管するファイルの正当性を保証するためのデータを集約し保証手続きを代行する集約サーバ１０４と、集約サーバ１０４が生成した正当性保証データを新聞に公表するなどの方法により保証する公開サーバ１０５が、インターネット１０１を介して接続されている。

【００１４】

このような構成により、本例のファイル保管システムでは、ＮＡＳサーバ１０３において格納するデータの存在時刻や非改ざん性を長期にわたって証明し、ファイルの保証を可能とする。すなわち、ＮＡＳサーバ１０３は、利用者用ＰＣ１０２からの要求を受けて、保証対象ファイルに対する保証データ（長期経過後にも保証要求時点から改竄されていないことを証明することができる証拠情報）を生成し、保証対象ファイルと共に保存する。

【００１５】

このように、保証データの生成処理を、ファイルを保存するＮＡＳサーバ１０３側で行うので、ＮＡＳ利用者にとっては負担が軽減される。また、ＮＡＳサーバ１０３にとっては、保証対象ファイルとそれに対する保証データとを一体で管理できるので管理が容易となる。

【００１６】

また、ＮＡＳサーバ１０３において生成される保証データは、公開サーバ１０５によって新聞公表等がなされたデータを含む。これにより、保証データの改竄は著しく困難になる。また、この困難性は、実社会との対応（例：新聞紙面に掲載された情報）によって達成されているため、たとえ、保証要求時点から長期経過後に、暗号ブレイク（暗号技術で利用される秘密情報の漏洩や、暗号解読技術の進歩など、何らかの原因によって暗号技術が危殆化すること）がおこったとしても尚、保証データの信頼性を確保することができる。

【００１７】

また、保証データ生成のために、ＮＡＳサーバ１０３が公開サーバ１０５を利用するときに、途中に集約サーバ１０４を設け、この集約サーバ１０４が、多数のＮＡＳサーバ１０３からの要求をまとめてデータサイズを削減し、公開サーバ１０５に送るようにする。これにより、公開サーバ１０５にとっては、処理の削減が可能となり、ＮＡＳサーバ１０３にとっては、直接公開サーバ１０５によって公開してもらう必要がなくなるため、コストが削減できる。さらに、集約サーバ１０４を設け、複数のＮＡＳサーバ１０３からの要求を集約することにより、複数のＮＡＳサーバ１０３における各処理間の相対的な時間的順序関係が証明可能となる。

【００１８】

以下、このようなファイル保管システムを構成する各装置の詳細を説明する。図１における利用者用ＰＣ１０２、ＮＡＳサーバ１０３、集約サーバ１０４、公開サーバ１０５のそれぞれは、ＣＰＵ（Central Processing Unit）や主メモリ、表示装置、入力装置、外部記憶装置からなるコンピュータ構成であり、光ディスク駆動装置等を介してＣＤ－ＲＯＭ等の記憶媒体に記録されたプログラムやデータを外部記憶装置内にインストールした後、この外部記憶装置から主メモリに読み込みＣＰＵで処理することにより、本発明に係わる各機能処理を実行する。

【００１９】

本例における利用者用ＰＣ１０２の構成は、基本的に、公知のＰＣ（パーソナルコンピュータ）と同様であり、利用者用ＰＣ１０２は、当該ＰＣ上のアプリケーションプログラム等で利用するファイルを作成し、それを、ネットワーク（インターネット１０１）を介し

て接続されたＮＡＳサーバ１０３に保存する。
【００２０】
また、利用者用ＰＣ１０２は、過去にＮＡＳサーバ１０３上に保存されたファイルを、必要に応じて、読み出したり、内容を変更して保存しなおしたり、追記したりすることができるようになっている。
【００２１】
さらに、本例における利用者用ＰＣ１０２には、ＮＡＳサーバ１０３に対し、あるファイルのその時点における状態（ファイル自体の内容や、ファイル名、作成者、作成日時、更新者、更新日時、属性、アクセス許可情報などのファイルに付随する管理情報）を将来にわたって証明可能な状態に保つ（以下、これを「ファイルの状態を固定する」と呼ぶ）ように要求する機能を有する。
【００２２】
また、本例におけるＮＡＳサーバ１０３は、インターネット１０１を介して接続された、一または複数の利用者用ＰＣから要求を受けて、利用者用ＰＣから受信したファイルを保存したり、保存されたファイルを読み出し、当該利用者用ＰＣに送信したりする。
【００２３】
さらに、ＮＡＳサーバ１０３は、利用者用ＰＣ１０２から要求を受けて、保存されたファイルの状態固定を行う。このファイルの状態固定にあたって、本例のＮＡＳサーバ１０３は、正当性保証を行うために、インターネット１０１を介して接続された集約サーバ１０４を利用する。
【００２４】
図６に示すように、ＮＡＳサーバ１０３には、ＣＰＵ２０１、ＲＡＭ２０２、不揮発性記憶部２０３、ストレージ装置２０４、ネットワークＩ／Ｆ２０５、ディスプレイ２０６、キーボード２０７が信号線を介して接続されている。
【００２５】
不揮発性記憶部２０３には、ファイルシステム管理プログラム２０８と、ＮＡＳサーバ署名用秘密鍵２０９が格納されている。
【００２６】
ＣＰＵ２０１は、不揮発性記憶部２０３に格納されたフィルシステム管理プログラム２０８等を、ＲＡＭ２０２上で実行し、機能として具現化する。
【００２７】
ストレージ装置２０４は、利用者用ＰＣ１０２から受信したファイルや、図１および図２，４に示すように、各ファイルに対応した連鎖データ１０１０～１０１３，１０２０～１０２２，１０３０～１０３２、および、ファイル固定保証データ１０５０等を保存する。
【００２８】
ネットワークＩ／Ｆ２０５は、利用者用ＰＣ１０２、集約サーバ１０４等の他のネットワーク（インターネット１０１）上のエンティティに対し、必要に応じて情報の送受信を行う。
【００２９】
図１に示す本例における集約サーバ１０４の構成は、基本的に図６に示したＮＡＳサーバ１０３と同様であり、この集約サーバ１０４は、ネットワーク（インターネット１０１）を介して接続された、一つまたは複数のＮＡＳサーバ（１０３）から受信した保証要求データ（１０１４）を元に、定期的に正当性保証データを生成し、それを公開サーバ１０５に送る。
【００３０】
さらに、各ＮＡＳサーバ（１０３）に対し、当該ＮＡＳサーバ（１０３）から受信した保証要求データから、公開サーバ１０５に送信した正当性保証データに至る、論理的な関係を保証する連鎖データを、ファイル固定保証データ１０５０として、送り返す。
【００３１】
集約サーバ１０４での、この連鎖データの生成には、例えば、特開２００１－３３１１０

４号公報、および、特開２００１－３３１１０５号公報に記載のヒステリシス署名技術を用いる。このヒステリシス署名技術は、署名作成の際、その時点までの署名履歴情報を反映させる技術であり、この技術では、作成した署名の署名情報を、作成する毎に、新たに署名履歴に追加する。これにより、作成した全ての署名は連鎖構造を持ち、検証の際は、署名に対する検証の他に、連鎖の検証も行うので、改竄は困難となる。

【００３２】

また、本例における公開サーバ１０５は、ネットワーク（インターネット１０１）を介して接続された、一つまたは複数の集約サーバ（１０４）から受信した正当性保証データ（１０５１）を、例えば、不特定多数の人が将来に渡り確認可能な状態にする（新聞、雑誌、ＷＥＢ、その他マスメディアに公表するなど）、大多数の利用者から信頼された機関に預託する（国、政府機関、公証人役場などが保証を行うなど）、当該正当性保証データに関係する利用者とは利害関係のない一人または複数の別の利用者に預託する等の方法により、将来にわたって当該正当性保証データ（１０５１）が、改竄されずに、ある時点で確かに存在したことを確認できるようにする。以下、これらの方法を総じて、単に「公表」と呼ぶ。尚、公開サーバ１０５の構成は、公表の方法に合わせて設計する。

【００３３】

これらの各サーバ（ＮＡＳサーバ１０３、集約サーバ１０４、公開サーバ１０５）による本発明に係わる動作を、図１を用いて説明する。

【００３４】

ＮＡＳサーバ１０３は、ストレージ装置２０４に、「ファイル１」、「ファイル２」、「ファイル３」を、それぞれが作成・更新等された時刻毎に、かつ、それぞれの時刻でのファイルを連鎖させるための連鎖用情報を付与して、連鎖データ１０１０～１０１３，１０２０～１０２２，１０３０～１０３２として保管している。

【００３５】

連鎖データ１０１０～１０１３，１０２０～１０２２，１０３０～１０３２における連鎖用情報は、例えば、図２の連鎖データ１０１１（「時刻Ｔ２におけるファイル１」）の連鎖用情報１０１１ａで示すように、前回保管した連鎖データ１０１０の連鎖用情報１０１０ａと「時刻Ｔ１におけるファイル１」１０１０ｂとに対して、例えばハッシュ関数をかけて求める。このようにして、ファイルの世代間の構造を形成する。

【００３６】

この状態で、利用者用ＰＣ１０２が、▲１▼「ファイル１の固定（時刻Ｔ４における現在の状態を証明可能な状態に保つ）」要求をＮＡＳサーバ１０３にすると、要求を受けたＮＡＳサーバ１０３は、当該連鎖データ１０１３をストレージ装置２０４から読み出し、図６に示すＮＡＳサーバ署名用秘密鍵２０９を用いて、▲２▼「ファイル１の最新情報に対しての署名」を行い、図３に詳細を示す保証要求データ１０１４を生成し、インターネット１０１を介して集約サーバ１０４に送出する。

【００３７】

保証要求データ１０１４は、図３に示すように、連鎖用データ１０１３ａおよび「時刻Ｔ４におけるファイル１」１０１３ｂからなる連鎖データ１０１３と、ＮＡＳ＿Ａの署名１０１４ａからなる。

【００３８】

このような保証要求データ１０１４を受信した集約サーバ１０４は、▲４▼「送られてきた保証要求データに対してヒステリシス署名を行い、定期的に、最新のヒステリシス署名を公開サーバ１０５に送る」。このように、集約サーバ１０４が公開サーバ１０５に送ったヒステリシス署名が正当性保証データとなる。

【００３９】

集約サーバ１０４で生成される連鎖データ１０５０は、図４に示すように、例えば、ＮＡＳサーバ１０３からの保証要求データ１０１４に集約サーバ１０４の秘密鍵による署名を付与し、さらに、一つ先の連鎖データの全体に対して例えばハッシュ関数をかけて算出したハッシュ値を、連鎖用前データとして付与した「ヒステリシス署名」となっている。ま

た、その最新のものが正当性保証データ１０５１となっている。
【００４０】
その後、集約サーバ１０４は、▲５▼「公開までの一連の連鎖データ（公開に至る集約サーバの連鎖データ１０５０）を当該ＮＡＳサーバ（１０３）に送り返す。
【００４１】
次に、図７から図１２を用いて、本例のファイル保管システムの処理動作を説明する。
【００４２】
図７は、図１におけるファイル保管システムのファイル作成処理動作例を示すシーケンス図であり、図８は、図１におけるファイル保管システムのファイル読み出し処理動作例を示すシーケンス図、図９は、図１におけるファイル保管システムのファイル書き込み処理動作例を示すシーケンス図、図１０は、図１におけるファイル保管システムのファイル状態固定処理の第１の動作例を示すシーケンス図、図１１は、図１におけるファイル保管システムのファイル状態固定処理の第２の動作例を示すシーケンス図、図１２は、図１におけるファイル保管システムのファイル状態固定検証処理動作例を示すシーケンス図である。
【００４３】
図７に示す例は、図１における利用者用ＰＣ１０２とＮＡＳサーバ１０３とによるファイル作成処理の処理フローを示したものである。ここでは、ファイル作成とは、ファイルを書き込むための領域確保や、ファイルに付随する管理情報を設定することとし、データの保存は含まないものとする。
【００４４】
尚、データの保存は、後述するファイル書き込み処理によって行われる。また、ファイル生成処理とファイル書き込み処理を続けて行うことにより、データの保存までを一括して行うようにしても良い。
【００４５】
以下、図７におけるファイル作成処理動作を説明する。
【００４６】
まず、ステップ３０１において、ＮＡＳ利用者用ＰＣ１０２における処理を開始し、ステップ３０２において、ＮＡＳサーバ１０３に対してファイル作成要求を出す。すなわち、ファイル名や作成者名などのファイルに付随する管理情報（ファイル付随情報）をＮＡＳサーバ１０３に送る。
【００４７】
以下、ＮＡＳサーバ１０３の処理に移り、まずステップ３０３において、ファイルに付随する管理情報（ファイル付随情報）とファイルの世代管理のための管理情報（ファイル世代管理情報）が格納される領域の設定を行い、設定した領域に、ＮＡＳ利用者用ＰＣ１０２から送られてきたファイル付随情報を書き込む。
【００４８】
次にステップ３０４において、ファイル内容自体（ファイル情報）とファイルの世代間の構造を形成するために用いられる情報（連鎖用情報）が格納される領域の設定を行い、設定した内容（各情報の格納領域のストレージ上の位置情報など）を、ファイル世代管理情報中の、世代番号「０」の欄に格納する。
【００４９】
そして、ステップ３０５において、ファイル世代管理情報中の、最新世代番号欄に「０」を設定し、ステップ３０６において、連鎖用データ初期値を生成し、ステップ３０４で設定した連鎖用情報領域に保存する。
【００５０】
さらに、ステップ３０７において、ファイル作成終了情報を返す。これに対応して、ステップ３０８において、ＮＡＳ利用者用ＰＣ１０２の処理を終了する。
【００５１】
次に、図８に基づき、本例における利用者用ＰＣ１０２とＮＡＳサーバ１０３とによるフ

ファイル読み出し処理動作を説明する。

【００５２】

まず、ステップ４０１において、ＮＡＳ利用者用ＰＣ１０２による「ファイル読み出し処理を開始し、ステップ４０２において、ＮＡＳ利用者用ＰＣ１０２からＮＡＳサーバ１０３に、ファイル読み出し要求を出す。尚、ここでは、対象ファイル名、読み出し要求者名などのファイルアクセス制御に必要な情報を送る。

【００５３】

以降、ＮＡＳサーバ１０３の処理に移り、まず、ステップ４０３において、対象ファイル名に対応するファイル付随情報の「アクセス許可情報」を参照し、当該アクセス（読み出し）を許可するかどうか判定する。許可しない場合は「読み出し失敗」をＮＡＳ利用者用ＰＣ１０２に返して処理を終わり、許可する場合は、ステップ４０４の処理に移る。

【００５４】

ステップ４０４での処理においては、ファイル世代管理情報を参照し、最新世代番号欄に書かれた世代のファイル情報の位置情報を取得する。そして、ステップ４０５において、先のステップ４０４で取得した位置情報に格納されたファイル情報を読み込み、利用者用ＰＣ１０２に送信する。

【００５５】

さらに、ステップ４０６において、必要があれば、ファイル付随情報を更新する。例えば、ファイル付随情報として「ファイルの最新読み出し時刻」があれば、当該「ファイルの最新読み出し時刻」を更新する。

【００５６】

その後、ステップ４０７に進み、ＮＡＳ利用者用ＰＣ１０２の処理を終了する。

【００５７】

次に、図９に基づき、本例における利用者用ＰＣ１０２とＮＡＳサーバ１０３とによるファイル書き込み処理動作を説明する。

【００５８】

まず、ステップ５０１において、ＮＡＳ利用者用ＰＣ１０２による「ファイル書き込み処理を開始し、ステップ５０２において、ＮＡＳ利用者用ＰＣ１０２からＮＡＳサーバ１０３に、ファイル書き込み要求を出す。尚、ここでは、対象ファイル名、書き込み要求者名などのファイルアクセス制御に必要な情報、および、書き込むデータを送る。

【００５９】

以降、ＮＡＳサーバ１０３の処理に移り、まず、ステップ５０３において、対象ファイル名に対応するファイル付随情報を参照し、当該アクセス（書き込み）を許可するかどうか判定する。許可しない場合は「書き込み失敗」をＮＡＳ利用者用ＰＣ１０２に返し、処理を終了する。

【００６０】

許可の場合には、ステップ５０４において、ファイル世代管理情報を参照し、最新世代番号欄に書かれた世代（第ｎ世代とする）のファイル情報と連鎖用情報の位置情報を取得する。そして、ステップ５０５において、第ｎ世代のファイル情報と連鎖用情報を読み込み、これらを結合し、そのハッシュ値を計算する。

【００６１】

さらに、ステップ５０６において、新しいファイル情報と連鎖用情報が格納される領域の設定を行い、設定された内容（各情報の格納領域のストレージ上の位置情報など）を、ファイル世代管理情報中の、世代番号「ｎ＋１」の欄に格納する。

【００６２】

その後、ステップ５０７において、先のステップ５０６で設定されたそれぞれの領域に、ＮＡＳ利用者用ＰＣ１０２から受信した書き込むべきデータ、および、ステップ５０５で計算したハッシュ値を書き込む。そして、ステップ５０８において、最新世代番号欄の値を「ｎ＋１」にする。

【００６３】

また、ステップ５０９において、必要があれば、ファイル付随情報を更新する。例えば、ファイル付随情報として「ファイルの最新読み出し時刻」があれば、当該「ファイルの最新読み出し時刻」を更新する。

【００６４】

その後、ステップ５１０に進み、ＮＡＳ利用者用ＰＣ１０２の処理を終了する。

【００６５】

次に、図１０に基づき、利用者用ＰＣ１０２とＮＡＳサーバ１０３および集約サーバ１０４と公開サーバ１０５とによるファイル状態固定処理における、利用者用ＰＣ１０２とＮＡＳサーバ１０３の処理動作を説明する。

【００６６】

まず、ステップ６０１において、ＮＡＳ利用者用ＰＣ１０２による「ファイル状態固定処理」を開始し、ステップ６０２において、ＮＡＳ利用者用ＰＣ１０２からＮＡＳサーバ１０３に、ファイル状態固定要求を出す。尚、ここでは、対象ファイル名、状態固定要求者名などのファイルアクセス制御に必要な情報を送る。

【００６７】

以降、ＮＡＳサーバ１０３の処理に移り、まず、ステップ６０３において、対象ファイル名に対応するファイル付随情報を参照し、当該アクセス（状態固定）を許可するかどうか判定する。許可しない場合は「状態固定失敗」をＮＡＳ利用者用ＰＣ１０２に返し、処理を終了する。

【００６８】

許可の場合には、ステップ６０４において、ファイル世代管理情報を参照し、最新世代番号欄に書かれた世代（第ｎ世代とする）のファイル情報と連鎖用情報の位置情報を取得する。そして、ステップ６０５において、第ｎ世代のファイル情報と連鎖用情報を読み込み、これらを結合し、そのハッシュ値を計算する。

【００６９】

さらに、ステップ６０６において、当該ファイルのファイル付随情報のハッシュ値を計算し、ステップ６０７において、ステップ６０５で計算したハッシュ値とステップ６０６で計算したハッシュ値を結合し、結合したものに対し、ＮＡＳサーバ１０３の署名用秘密鍵を用いて、ディジタル署名を生成する。このように、２つのハッシュ値を結合したものと生成されたディジタル署名とからなるデータが、図３示す「保証要求データ１０１４」である。

【００７０】

その後、ステップ６０８において、集約サーバ１０４に、当該保証要求データ１０１４を送り、集約サーバ１０４からファイル固定保証データ（１０５０）が送られてくるまで待つ。

【００７１】

集約サーバ１０４から、ファイル固定保証データ（１０５０）が送られてきたら、ステップ６０９において、当該ファイル固定保証データ（１０５０）を格納するための領域の設定を行い、設定した内容（領域のストレージ上の位置情報など）を、ファイル世代管理情報中の、世代番号ｎの欄に格納する。

【００７２】

そして、ステップ６１０において、先のステップ６０９で設定した領域に、集約サーバ１０４から送られてきたファイル固定保証データ（１０５０）を書き込み、ステップ６１１において、処理を終了する。

【００７３】

次に、図１１に基づき、利用者用ＰＣ１０２とＮＡＳサーバ１０３および集約サーバ１０４と公開サーバ１０５とによるファイル状態固定処理における、集約サーバ１０４の処理動作を説明する。

【００７４】

まず、ステップ７０１において、「ファイル状態固定処理」を開始し、ステップ７０２に

おいて、公開時刻（例：一週間毎）であるか否かを判別し、公開時刻になれば、ステップ７０８以降の処理に進み、公開時刻でなければ、ステップ７０３以降の「ヒステリシス署名」処理に進む。

【００７５】

ステップ７０３においては、ＮＡＳサーバ１０３から保証要求データが送られて来たか否を判別し、来ればステップ７０４の処理に進み、来なければステップ７０２の処理に戻る。

【００７６】

ステップ７０４においては、予め保持してある最新（第Ｍ番目とする）の署名記録を取得し、そのハッシュ値を計算し、新たな連鎖用前データとする。そして、ステップ７０５において、連鎖用前データと保証要求データを連結し、署名対象データとする。

【００７７】

その後、ステップ７０６において、この署名対象データに対し、集約サーバ１０４の署名用秘密鍵を用いて署名し、ステップ７０７において、連鎖用前データ、保証要求データ、署名を、第Ｍ＋１番目の署名記録として保存し、ステップ７０２の処理に戻る。

【００７８】

先のステップ７０２での公開時刻（例：一週間毎）の判別処理で、公開時刻になれば、まず、ステップ７０８において、その時点で最新の署名記録（第Ｍ＿Ｘ番目とする）を取得してハッシュ値を計算し、新たな連鎖用前データとする。

【００７９】

そして、ステップ７０９において、公開用データ（例：公開時刻、公開サーバ名、集約サーバ名等を含むデータ）を作成し、連鎖用前データと連結して、署名対象データとし、ステップ７１０において、その署名対象データに対し、集約サーバ１０４の署名用秘密鍵を使って署名する。

【００８０】

その後、ステップ７１１において、連鎖用前データ、公開用データ、署名を連結し、「正当性保証データ（１０５１）」として公開サーバ１０５に送る。

【００８１】

さらに、ステップ７１２において、第ｉ番目（１≦ｉ≦Ｍ＿Ｘ）の署名記録に対応するＮＡＳサーバ（例えば、第ｉ番目の署名記録に含まれる保証要求データ１０１４を送ってきたＮＡＳサーバ１０３）に対し、第ｉ番目から第Ｍ＿Ｘ番目までの署名記録と正当性保証データ（１０５１）を結合したものを、ファイル固定保証データ（１０５０）として、送り返す。

【００８２】

そして、ステップ７１３において、最新の署名記録番号を第０番とし、第０番目の署名記録の初期値をランダムに生成して保存し、ステップ７０２での処理に戻る。

【００８３】

次に、図１２に基づき、本例における利用者用ＰＣ１０２によるファイル状態固定検証処理の処理動作を説明する。尚、ここでは、利用者用ＰＣ１０２において検証処理を行う例を示しているが、これと異なっていても良い。

【００８４】

例えば、調停機関が、ＮＡＳサーバ１０３の利用者の主張の正当性を調べる目的で、ＮＡＳサーバ１０３から証拠としてファイル状態固定検証に必要なデータの提出を受け、ファイル状態固定検証処理を行っても良い。この場合でも処理手順は、図１２と同様で良い。

【００８５】

まず、ステップ８０１において、「ファイル状態固定検証処理」を開始し、ステップ８０２において、ＮＡＳサーバ１０３から、固定されたファイル（その世代のファイル情報と、連鎖用情報と、ファイル付随情報を含む）と、それに対するファイル固定保証データ（１０５０）を取得する。

【００８６】

次に、ステップ８０３において、ファイル固定保証データ（１０５０）に含まれる、保証要求データ（１０１４）を、ＮＡＳサーバ１０３の公開鍵を使った署名検証処理により検証できることを確認する（公知のディジタル署名検証処理を行えば良い）。確認されなければステップ８０９へ進み、「検証失敗」となる。

【００８７】

検証できれば、ステップ８０４において、保証要求データ（１０１４）が、ステップ６０５、６０６で計算されたハッシュ値を含むことを確認する。確認されなければステップ８０９へ進み、「検証失敗」となる。

【００８８】

確認できればステップ８０５において、ファイル固定保証データ（１０５０）に含まれる、正当性保証データ（１０５１）が、公開サーバ１０５によって実際に公表されている（例：新聞公表など）ことを確認する。確認されなければステップ８０９へ進み、「検証失敗」となる。

【００８９】

公表が確認できればステップ８０６において、ファイル固定保証データ（１０５０）に含まれる各署名記録（署名対象データと署名の組。ただし、署名対象データは連鎖用前データと保証要求データからなる）を集約サーバ１０４の公開鍵を使って検証する。検証できなければステップ８０９へ進み、「検証失敗」となる。

【００９０】

検証できればステップ８０７において、ファイル固定保証データ（１０５０）に含まれる署名記録間の連鎖関係を確認する。すなわち、各署名記録に含まれる連鎖用前データ（署名対象データに含まれる）が、一つ前の署名記録（署名対象データと署名）のハッシュ値と一致することを確認する。確認できなければステップ８０９へ進み、「検証失敗」となり、確認できれば、ステップ８０８に進み、「検証成功」と出力して処理を終了する。

【００９１】

以上、図１～図１２を用いて説明したように、本例では、ＮＡＳサーバ１０３の利用者は、自身が状態を固定したいと思ったファイルがある場合、ＮＡＳ利用者用ＰＣ１０２を用いて、インターネット１０１で接続されたＮＡＳサーバ１０３に対して、固定要求を出すことにより、要求時点での当該ファイルの内容や付帯状況（作成者、作成日時、更新者、更新日時、属性、アクセス許可情報、など）を長期間証明可能な証拠情報（ファイル固定保証データ１０５０）が生成され、当該ファイルと共にＮＡＳサーバ１０３内に保存されるため、長期間に渡り安全にファイルの状態固定が可能となる。ＣＤ－Ｒ等の物理的なメディアに格納する従来の技術とは異なり、特別な装置は必要としない。

【００９２】

また、本例によれば、ＮＡＳサーバ１０３の運用者は、利用者に対して、ファイル固定サービスを提供することが可能となる。本例では、ＮＡＳサーバ１０３が、利用者からの要求に応じて、要求時におけるファイルの状態を固定する、すなわち、当該ファイルに対するファイル固定保証データを生成し当該ファイルと共に管理することが可能となる。

【００９３】

このファイル固定保証データは、その一部が、公開サーバ１０５によって公表されたデータと一致していること、さらに、ファイル固定保証データ自体の一貫性が保たれていること（ファイル固定保証データの構成が、予め決められた条件を満たしていること）の確認により、改竄されていないことがわかる。従って、固定要求時から長期経過後であっても、ファイルの状態がどのような状態であったかを証明可能である。

【００９４】

この証明可能性は、ＮＡＳサーバ１０３の生成したディジタル署名だけに基づいているわけではないので、例えば、ＮＡＳサーバ１０３が秘密裏に保持すべき署名用秘密鍵が漏洩した場合であっても、なお保たれる。

【００９５】

さらに、本例では、利用者のファイルを、ファイルごとに変更履歴も含め、改竄が著しく

困難になるように、ファイル作成時から最終変更時まで連鎖構造を形成しながら管理されている。従って、固定要求時におけるファイルの状態だけでなく、固定された状態に至る当該ファイルの変更履歴についても、同様に、連鎖関係を確認することによって、証明可能である。

【００９６】

また、本例によれば、集約サーバ１０４は、複数のＮＡＳサーバ（１０３）からの保証要求データを受け付けることができるので、ＮＡＳサーバごとに公表を行う必要はなく、効率的である。

【００９７】

さらに、集約サーバ１０４は、特開２００１－３３１１０４号公報、および、特開２００１－３３１１０５号公報等に開示された、履歴情報を利用したディジタル署名方法（「ヒステリシス署名」）を用いて、各ＮＡＳサーバからの保証要求データに対し署名を生成するので、集約サーバ１０４の署名用秘密鍵の漏洩に対しても耐性を有し（例えば．署名の有効性を証明できる）、また、各保証要求データ間の時間的順序関係を示すことが可能となる。

【００９８】

さらに、本例では、ヒステリシス署名によって形成された署名履歴の一部を、正当性保証データとして公開サーバ１０５に送った後、各ＮＡＳサーバに対し、当該ＮＡＳサーバ（１０３）からの保証要求データ１０１４から、公開サーバ１０５に送った正当性保証データ１０５１に至る一連の連鎖を、ファイル固定保証データ（１０５０）として送り返すことにより、ファイルの状態を、集約サーバ１０４への問い合わせなしに証明することができる。

【００９９】

このようにして、本例では、ＮＡＳサーバ１０３に保管されたファイルを、その時点における状態を証明可能な状態にし、将来に渡り有効な証拠情報を構築可能な、安全性の高いストレージシステムを提供できる。

【０１００】

尚、本発明は、図１～図１２を用いて説明した例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、本例では、ファイルごとに連鎖構造を形成するようにしていた、すなわち、ファイル間の連鎖形成用データは、当該ファイルの直前の状態に基づき生成されていたが、これとは異なり、同一利用者の他のファイルや他の利用者のファイルのその時点における最新状態が反映されるようにしても良い。このようにすることにより、複数のファイル間での時間的な前後関係が明確になる。また、不正を試みようとするものにとっては、他のファイルとの整合性をも考慮しなければならないので、安全性がさらに向上する。

【０１０１】

また、集約サーバ１０４を設けず、ＮＡＳサーバ１０３から直接、公開サーバ１０５に最新の保存ファイルデータ（保証要求データ１０１４）を送り、公表を依頼する構成としても良い。

【０１０２】

また、ＮＡＳサーバ１０３においても、集約サーバ１０４と同様に、各連鎖データを、ヒステリシス履歴に基づき管理する構成としても良い。

【０１０３】

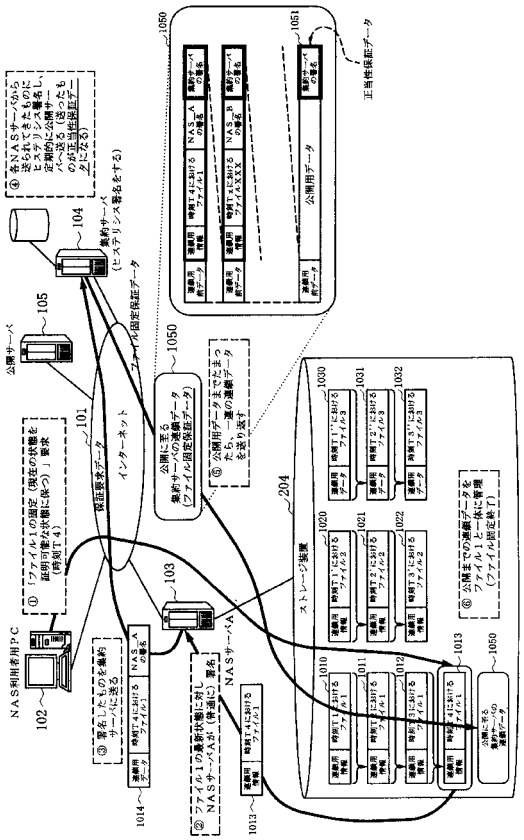
また、本例では、ネットワークとしてインターネット１０１を用いた構成としているが、例えば、ＬＡＮやＷＡＮ（Wide Area Network）等によるネットワーク構成としても良い。

【０１０４】

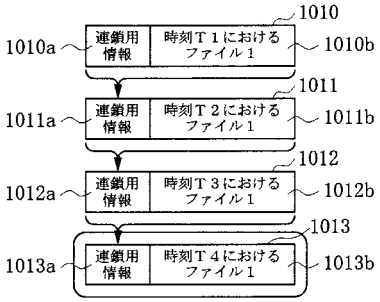
また、本例の各サーバのコンピュータ構成において、光ディスクを記録媒体として用いているが、ＦＤ（Flexible Disk）等を記録媒体として用いることでも良い。また、プログラムのインストールに関しても、通信装置を介してネットワーク経由でプログラムをダウ

ンロードしてインストールすることでも良い。
【０１０５】
【発明の効果】
本発明によれば、利用者からのファイル状態の固定要求に応じ、ＮＡＳサーバ等のネットワーク上のストレージサーバにおいて、公開サーバ等によって公表されたデータを含むファイル固定保証データを生成し、当該ファイルと関連付けて保存するので、利用者の要求時点における状態を、長期間に渡り安全に証明でき、利用者にとって負担が少ない、ストレージシステムを提供することが可能となる。
【図面の簡単な説明】
【図１】本発明に係わるディジタルデータ保管システムの構成例を示すブロック図である。
【図２】図１におけるＮＡＳサーバ１０３で生成される連鎖データの構成例を示す説明図である。
【図３】図１におけるＮＡＳサーバ１０３から集約サーバ１０４に送信される保証要求データの構成例を示す説明図である。
【図４】図１におけるＮＡＳサーバ１０３で保持するファイル固定保証データの構成例を示す説明図である。
【図５】図１におけるディジタルデータ保管システムの概略構成例を示すブロック図である。
【図６】図１におけるＮＡＳサーバ１０３の構成例を示すブロック図である。
【図７】図１におけるファイル保管システムのファイル作成処理動作例を示すシーケンス図である。
【図８】図１におけるファイル保管システムのファイル読み出し処理動作例を示すシーケンス図である。
【図９】図１におけるファイル保管システムのファイル書き込み処理動作例を示すシーケンス図である。
【図１０】図１におけるファイル保管システムのファイル状態固定処理の第１の動作例を示すシーケンス図である。
【図１１】図１におけるファイル保管システムのファイル状態固定処理の第２の動作例を示すシーケンス図である。
【図１２】図１におけるファイル保管システムのファイル状態固定検証処理動作例を示すシーケンス図である。
【符号の説明】
１０１：インターネット、１０２：利用者用ＰＣ、１０３：ＮＡＳサーバ、１０４：集約サーバ、１０５：公開サーバ、２０１：ＣＰＵ、２０２：ＲＡＭ、２０３：不揮発性記憶部、２０４：ストレージ装置、２０５：ネットワークＩ／Ｆ、２０６：ディスプレイ、２０７：キーボード、２０８：ファイルシステム管理プログラム，２０９：ＮＡＳサーバ署名用秘密鍵、１０１０～１０１３，１０２０～１０２２，１０３０～１０３２：連鎖データ、１０１０ａ～１０１３ａ，１０２０ａ～１０２２ａ，１０３０ａ～１０３２ａ：連鎖用情報、１０１０ｂ：時刻Ｔ１におけるファイル１、１０１１ｂ：時刻Ｔ２におけるファイル１、１０１２ｂ：時刻Ｔ３におけるファイル１、１０１３ｂ：時刻Ｔ４におけるファイル１、１０１４：保証要求データ、１０１４ａ：ＮＡＳ＿Ａの署名、１０５０：ファイル固定保証データ（「公開に至る集約サーバの連鎖データ」）、１０５１：正当性保証データ。

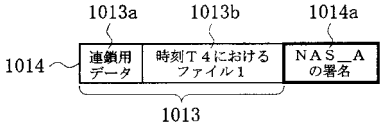
【図１】


NAS利用者用PC
102
公開サーバ
105
インターネット
101
NASサーバ
103
集約サーバ
（ヒステリシス署名をする）
104
ファイル固定保証データ
保証要求データ
ストレージ装置
204
NASサーバA
正当性保証データ
1050
1051
1010
1011
1012
1013
1014
1020
1021
1022
1030
1031
1032
連鎖用前データ
連鎖用情報
公開用データ
NAS_Aの署名
集約サーバの署名
時刻T1におけるファイル1
時刻T2におけるファイル1
時刻T3におけるファイル1
時刻T4におけるファイル1
時刻T2におけるファイル2
時刻T3におけるファイル2
時刻T3におけるファイル3
① 「ファイル1の固定（現在の状態を証明可能な状態に保つ）」要求
② ファイル1の最新状態に対しNASサーバAが（検証に）署名
③ 署名したものを集約サーバに送る
④ 各NASサーバから送られてきたものにヒステリシス署名をし、定期的に公開サーバへ送る（送ったものが正当性保証データとなる）
⑤ 公開用データまでたまったら、一連の連鎖データを送り返す
⑥ 公開までの連鎖データをファイル1と共に署名（ファイル固定完了）
公開に至る集約サーバへの連鎖データ（ファイル固定保証データ）

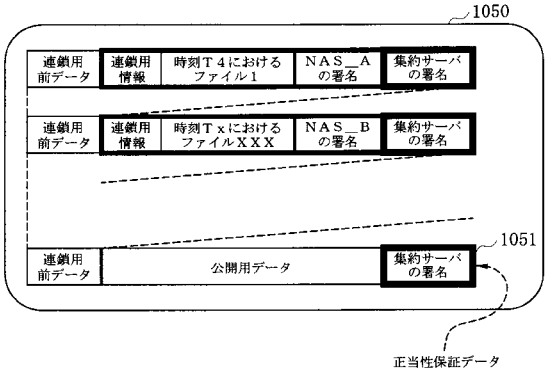
【図２】


1010
1010a
連鎖用情報
時刻Ｔ１における
ファイル１
1010b
1011
1011a
連鎖用情報
時刻Ｔ２における
ファイル１
1011b
1012
1012a
連鎖用情報
時刻Ｔ３における
ファイル１
1012b
1013
1013a
連鎖用情報
時刻Ｔ４における
ファイル１
1013b

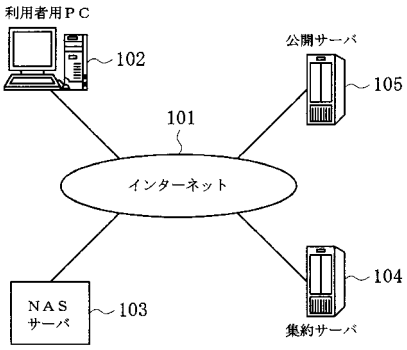
【図３】


1013a
1013b
1014a
1014
連鎖用データ
時刻Ｔ４における
ファイル１
ＮＡＳ＿Ａ
の署名
1013

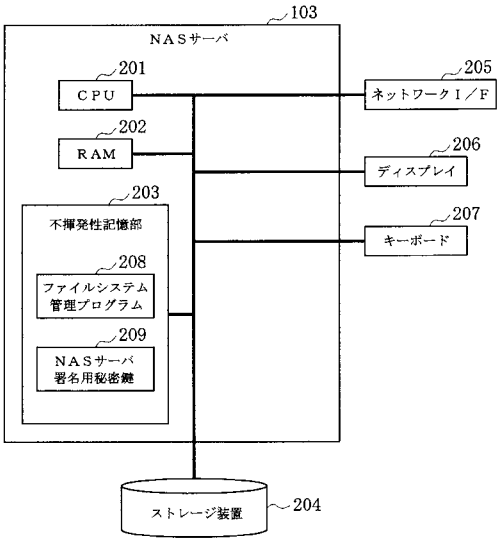
【図４】


1050
連鎖用前データ
連鎖用情報
時刻Ｔ４における
ファイル１
ＮＡＳ＿Ａ
の署名
集約サーバ
の署名
連鎖用前データ
連鎖用情報
時刻Ｔｘにおける
ファイルＸＸＸ
ＮＡＳ＿Ｂ
の署名
集約サーバ
の署名
連鎖用前データ
公開用データ
集約サーバ
の署名
1051
正当性保証データ

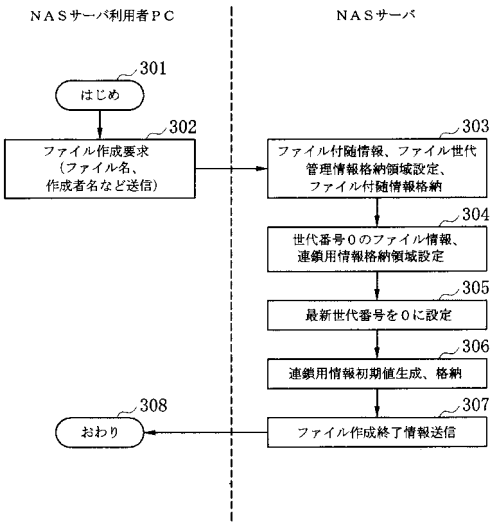
【図５】


利用者用ＰＣ
102
公開サーバ
105
101
インターネット
104
集約サーバ
ＮＡＳ
サーバ
103

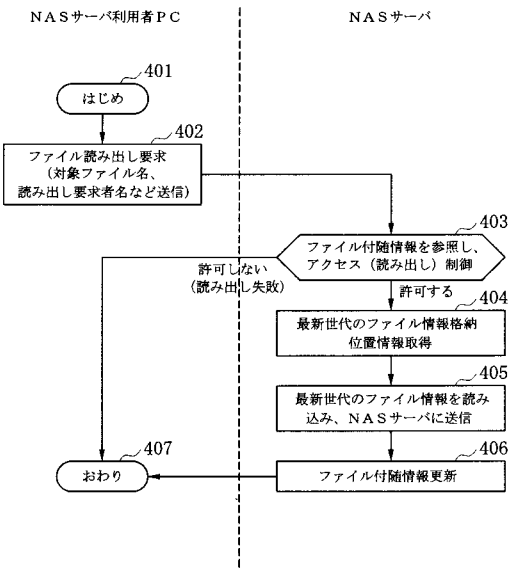
【図６】


103
NASサーバ
201
CPU
202
RAM
203
不揮発性記憶部
208
ファイルシステム
管理プログラム
209
NASサーバ
署名用秘密鍵
205
ネットワークI／F
206
ディスプレイ
207
キーボード
ストレージ装置
204

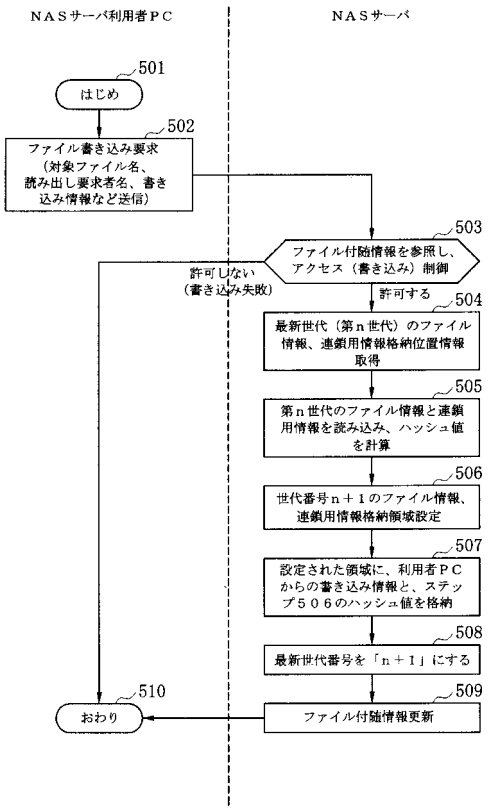
【図７】


NASサーバ利用者PC
NASサーバ
301
はじめ
302
ファイル作成要求
（ファイル名、
作成者名など送信）
303
ファイル付随情報、ファイル世代
管理情報格納領域設定、
ファイル付随情報格納
304
世代番号0のファイル情報、
連鎖用情報格納領域設定
305
最新世代番号を0に設定
306
連鎖用情報初期値生成、格納
307
ファイル作成終了情報送信
308
おわり

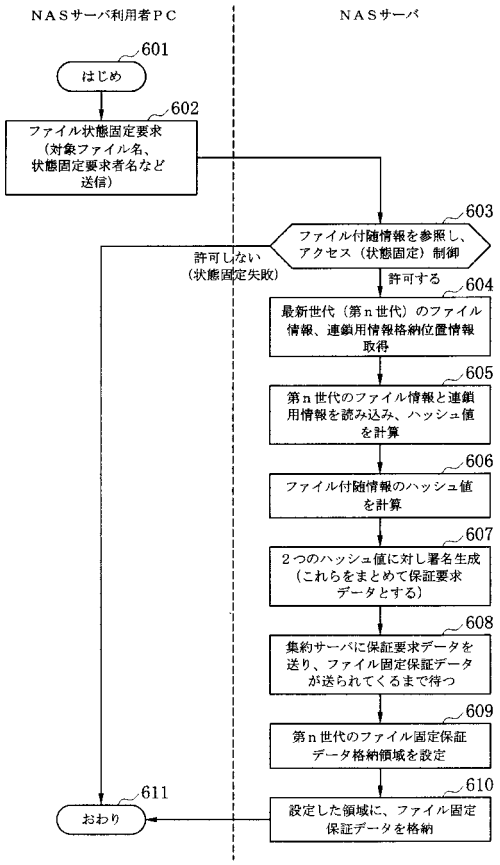
【図８】


NASサーバ利用者PC
NASサーバ
401
はじめ
402
ファイル読み出し要求
（対象ファイル名、
読み出し要求者名など送信）
403
ファイル付随情報を参照し、
アクセス（読み出し）制御
許可しない
（読み出し失敗）
許可する
404
最新世代のファイル情報格納
位置情報取得
405
最新世代のファイル情報を読み
込み、NASサーバに送信
406
ファイル付随情報更新
407
おわり

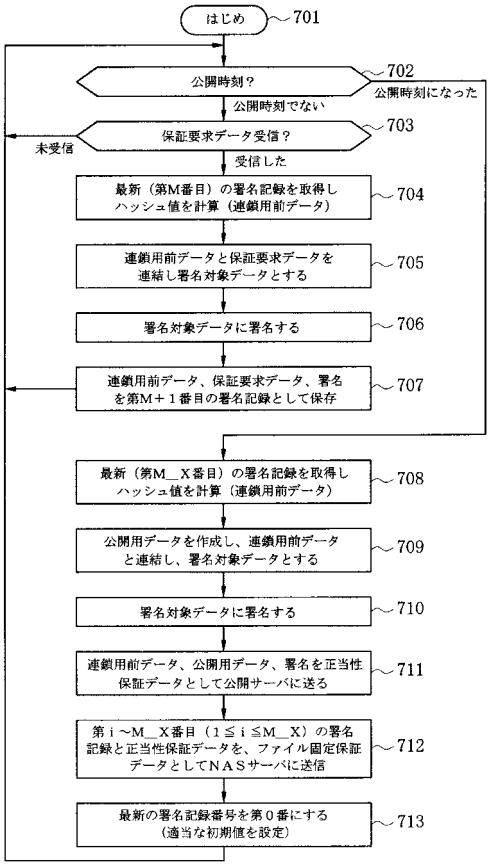
【図９】


NASサーバ利用者PC
NASサーバ
501
はじめ
502
ファイル書き込み要求
（対象ファイル名、
読み出し要求者名、書き
込み情報など送信）
503
ファイル付随情報を参照し、
アクセス（書き込み）制御
許可しない
（書き込み失敗）
許可する
504
最新世代（第n世代）のファイル
情報、連鎖用情報格納位置情報
取得
505
第n世代のファイル情報と連鎖
用情報を読み込み、ハッシュ値
を計算
506
世代番号n＋1のファイル情報、
連鎖用情報格納領域設定
507
設定された領域に、利用者PC
からの書き込み情報と、ステッ
プ５０６のハッシュ値を格納
508
最新世代番号を「n＋1」にする
509
ファイル付随情報更新
510
おわり

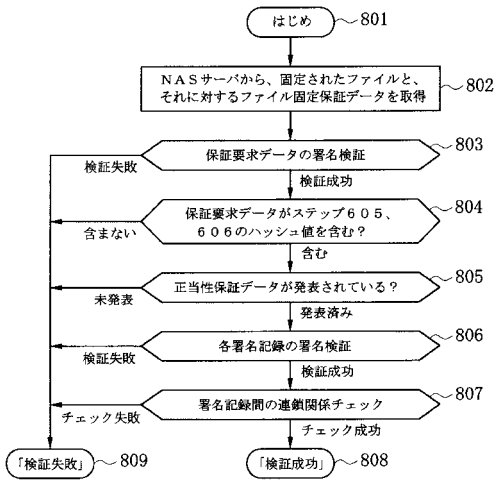
【図１０】


ＮＡＳサーバ利用者ＰＣ
ＮＡＳサーバ
601
はじめ
602
ファイル状態固定要求
（対象ファイル名、
状態固定要求者名など
送信）
603
ファイル付随情報を参照し、
アクセス（状態固定）制御
許可しない
（状態固定失敗）
許可する
604
最新世代（第ｎ世代）のファイル
情報、連鎖用情報格納位置情報
取得
605
第ｎ世代のファイル情報と連鎖
用情報を読み込み、ハッシュ値
を計算
606
ファイル付随情報のハッシュ値
を計算
607
２つのハッシュ値に対し署名生成
（これらをまとめて保証要求
データとする）
608
集約サーバに保証要求データを
送り、ファイル固定保証データ
が送られてくるまで待つ
609
第ｎ世代のファイル固定保証
データ格納領域を設定
610
設定した領域に、ファイル固定
保証データを格納
611
おわり

【図１１】


はじめ
701
公開時刻？
702
公開時刻になった
公開時刻でない
保証要求データ受信？
703
未受信
受信した
最新（第Ｍ番目）の署名記録を取得し
ハッシュ値を計算（連鎖用前データ）
704
連鎖用前データと保証要求データを
連結し署名対象データとする
705
署名対象データに署名する
706
連鎖用前データ、保証要求データ、署名
を第Ｍ＋１番目の署名記録として保存
707
最新（第Ｍ＿Ｘ番目）の署名記録を取得し
ハッシュ値を計算（連鎖用前データ）
708
公開用データを作成し、連鎖用前データ
と連結し、署名対象データとする
709
署名対象データに署名する
710
連鎖用前データ、公開用データ、署名を正当性
保証データとして公開サーバに送る
711
第ｉ～Ｍ＿Ｘ番目（１≦ｉ≦Ｍ＿Ｘ）の署名
記録と正当性保証データを、ファイル固定保証
データとしてＮＡＳサーバに送信
712
最新の署名記録番号を第０番にする
（適当な初期値を設定）
713

【図１２】


はじめ
801
ＮＡＳサーバから、固定されたファイルと、
それに対するファイル固定保証データを取得
802
保証要求データの署名検証
803
検証失敗
検証成功
保証要求データがステップ６０５、
６０６のハッシュ値を含む？
804
含まない
含む
正当性保証データが発表されている？
805
未発表
発表済み
各署名記録の署名検証
806
検証失敗
検証成功
署名記録間の連鎖関係チェック
807
チェック失敗
チェック成功
「検証失敗」
809
「検証成功」
808

フロントページの続き

(72)発明者 大本 周広
東京都江東区新砂一丁目６番２７号 株式会社日立製作所公共システム事業部内
(72)発明者 別所 良治
東京都江東区新砂一丁目６番２７号 株式会社日立製作所公共システム事業部内

審査官 平井 誠

(56)参考文献 特開２００１－３３１１０４（ＪＰ，Ａ）
原田 篤史 Atsushi Harada,他３名，電子カルテ管理方式 An electric medical record，コンピュータセキュリティシンポジウム２００１ Computer Security Symposium 2001，日本，社団法人情報処理学会 Information Processing Society of Japan，２００１年１０月３１日，Ｎｏ．１５，7頁－１２頁
宇根 正志 Masashi Une，連鎖型タイムスタンプの検証に用いられる情報の管理 Management of Information Used to Verify Time Stamps in Linking Schemes，コンピュータセキュリティシンポジウム２０００ Computer Security Symposium 2000，日本，社団法人情報処理学会 Information Processing Society of Japan，２０００年１０月２６日，第2000巻，２５頁－３０頁
洲崎 誠一 Seiichi Susaki，暗号ブレイク対応電子署名アリバイ実現機構（その２）－詳細方式－ Alibi Establishment for Electronic Signatures:How to prove that you did not make the electronic signature in question even when the base cryptosystem was collapsed Part 2. Concrete Schemes and Evaluation，情報処理学会研究報告 Ｖｏｌ．２０００ Ｎｏ．３０ IPSJ SIG Notes，日本，社団法人情報処理学会 Information Processing Society of Japan，２０００年 3月２１日，第2000巻，１９項－２４項

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24