

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4141069号

(P4141069)

(45) 発行日 平成20年8月27日 (2008. 8. 27)

(24) 登録日 平成20年6月20日 (2008. 6. 20)

(51) Int. Cl.

F I

G O 6 F 21/24 (2006. 01)

G O 6 F 12/14 5 6 O D

G O 6 F 3/06 (2006. 01)

G O 6 F 3/06 3 O 4 H

請求項の数 6 (全 24 頁)

(21) 出願番号	特願平11-267816	(73) 特許権者	000006747
(22) 出願日	平成11年9月21日 (1999. 9. 21)		株式会社リコー
(65) 公開番号	特開2000-148597 (P2000-148597A)		東京都大田区中馬込 1 丁目 3 番 6 号
(43) 公開日	平成12年5月30日 (2000. 5. 30)	(74) 代理人	100089118
審査請求日	平成16年11月24日 (2004. 11. 24)		弁理士 酒井 宏明
(31) 優先権主張番号	09/167629	(72) 発明者	テツロウ モトヤマ
(32) 優先日	平成10年10月6日 (1998. 10. 6)		アメリカ合衆国, カリフォルニア州 9 5
(33) 優先権主張国	米国 (US)		1 3 4 - 8 8 0 0, サン ホセ, オーチャ
			ード パークウェイ ドライブ 3 0 0 1
			, リコー コーポレーション エス・ピー
			・ピー内
		(72) 発明者	谷内田 益義
			東京都大田区中馬込 1 丁目 3 番 6 号 株式
			会社リコー内

最終頁に続く

(54) 【発明の名称】 データの保存方法、データストレージユニットおよびコンピュータ読み取り可能な記録媒体

(57) 【特許請求の範囲】

【請求項 1】

不揮発性ストレージデバイスにデータを保存するデータストレージユニットのデータの保存方法であって、

前記データストレージユニットは、

前記データストレージユニットに対する許可のないアクセスを検出するセンサと、

前記不揮発性ストレージデバイスおよび前記センサを制御する処理ユニットと、

電源に障害が発生した場合に、前記不揮発性ストレージデバイスと、前記センサと、前記処理ユニットとに対して電力を供給可能なバックアップ電源と、を備え、

前記処理ユニットは、前記電源に障害が発生した場合に、

前記バックアップ電源から前記データストレージユニットへの電力の供給を開始する工程と、

前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを禁止する工程と、

前記センサにより前記データストレージユニットに対するアクセスを検出する工程と、

前記データストレージユニットに対するアクセスが検出された場合に、所定の値を前記不揮発性ストレージデバイスに保存されている前記データに上書きすることによって前記不揮発性ストレージデバイスに保存されている前記データを消去する工程と、

を含むことを特徴とするデータの保存方法。

【請求項 2】

10

20

前記処理ユニットが、さらに、前記電源が回復した後、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを許可する工程を含むことを特徴とする請求項1に記載のデータの保存方法。

【請求項3】

不揮発性ストレージデバイスにデータを保存するデータストレージユニットであって、前記データストレージユニットに対する許可のないアクセスを検出するセンサと、前記不揮発性ストレージデバイスおよび前記センサを制御する処理ユニットと、電源に障害が発生した場合に、前記不揮発性ストレージデバイスと、前記センサと、前記処理ユニットとに対して電力を供給可能なバックアップ電源と、を備え、

前記処理ユニットは、前記電源に障害が発生した場合に、前記バックアップ電源から前記データストレージユニットへの電力の供給を開始し、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを禁止し、

前記センサにより前記データストレージユニットに対するアクセスを検出し、前記データストレージユニットに対するアクセスが検出された場合に、所定の値を前記不揮発性ストレージデバイスに保存されている前記データに上書きすることによって前記不揮発性ストレージデバイスに保存されている前記データを消去することを特徴とするデータストレージユニット。

【請求項4】

前記処理ユニットは、さらに、前記電源が回復した後、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを許可することを特徴とする請求項3に記載のデータストレージユニット。

【請求項5】

不揮発性ストレージデバイスにデータを保存するデータストレージユニットに前記データを保存するための一以上の命令の一以上のシーケンスを有するコンピュータ読み取り可能な記録媒体であって、

前記データストレージユニットは、前記データストレージユニットに対する許可のないアクセスを検出するセンサと、前記不揮発性ストレージデバイスおよび前記センサを制御する処理ユニットと、電源に障害が発生した場合に、前記不揮発性ストレージデバイスと、前記センサと、前記処理ユニットとに対して電力を供給可能なバックアップ電源と、を備え、

前記一以上の命令の一以上のシーケンスは、一以上のプロセッサによって実行される場合に、前記一以上のプロセッサに対し、

前記処理ユニットが、前記電源に障害が発生した場合に、前記バックアップ電源から前記データストレージユニットへの電力の供給を開始する手順と、

前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを禁止する手順と、

前記センサにより前記データストレージユニットに対するアクセスを検出する手順と、前記データストレージユニットに対するアクセスが検出された場合に、所定の値を前記不揮発性ストレージデバイスに保存されている前記データに上書きすることによって前記不揮発性ストレージデバイスに保存されている前記データを消去する手順と、

を実行させる命令を含むことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項6】

前記処理ユニットが、さらに、前記データストレージユニットに対する電源が回復した後、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを許可する手順を実行させる命令を含むことを特徴とする請求項5に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

10

20

30

40

50

【発明の属する技術分野】

本発明はデータストレージシステムに関し、より詳細には、ファイルの保全性および安全性を保証する、データの保存技術に関する。

【0002】**【従来の技術および発明が解決しようとする課題】**

大部分のコンピュータシステムは、データを保存・保持するために任意の種類の不揮発性ストレージ (non-volatile storage) を含んでいる。不揮発性ストレージは、電源がオフにされた場合であっても、その保存内容を保持することが可能な記憶媒体を提供するものである。なお、不揮発性ストレージの一般的な例には、フロッピー・ディスク、ハードディスクおよびテープ等が含まれる。

10

【0003】

大部分の種類の不揮発性ストレージは、特に冗長ストレージ (redundant storage) が使用される場合に比較的高い信頼性を提供する。また、不揮発性ストレージの性能は、不揮発性ストレージの種類に応じて大きく変化する。たとえばハードディスクは、従来より、アクセススピードの点においてフロッピー・ディスクやテープより高い性能を示す。また、不揮発性ストレージにデータを保存する際に使用されるプロセスは一般的に非破壊的なもの (たとえば記憶媒体を破壊して情報を保存するものではない) であるため、大部分の種類の不揮発性ストレージについては再利用することが可能である (たとえば、データを何度も書き込むことが可能)。

【0004】

20

ところで、データファイル形式のデータを不揮発性ストレージから削除しようとする場合、不揮発性ストレージにおいてはデータファイルに関連するディレクトリ情報が単に更新されるだけであり、データファイルそのものは変更されていないことが通常である。たとえば、多くのコンピュータシステム上におけるデータファイルの削除処理は、ファイルディレクトリまたはファイルアロケーションテーブルからファイル名を削除することによって実行される。これにより、他のデータを保存するために利用されるデータファイルで占有可能な記憶位置が作成される。

【0005】

しかしながら、そのデータファイルは不揮発性ストレージ上に未だ存在しており、他のデータをそのデータファイルに上書してしまわない限り、そのデータファイルは回復可能な状態にある。したがって、このアプローチは、特定のデータのコピーがオリジナルコピー (原本) であるか否かを知ることが困難になると共に、第三者によるデータの取得行為に対してデータを無抵抗なものにしてしまう。

30

【0006】

さらに、別の種類の不揮発性ストレージとして、データの書き込みは1回だけであるが、必要な回数読み出しできるようにしたものがある。この種類の不揮発性ストレージは、通常、WORM (write once, read many) 記憶媒体と呼ばれている。このWORM不揮発性ストレージデバイスの一般的な例としては、光ディスクがある。この種類の記憶媒体は、たとえば医学的な記録やビジネスの記録のように一度だけ書き込まれ、複数回読み出されることがあるようなデータをアーカイブするために有効である。したがって、WORM不揮発性ストレージデバイスにおいては、データの更新または上書きが不可能であることから、特定のデータのコピーがオリジナルコピー (原本) であるということが保証される。

40

【0007】

しかしながら、WORMシステムおよび従来のリード／ライト (読み出し／書き込み) ストレージシステムには、データの変更に対して無防備であるという不都合な点がある。あるデータのユーザにとっては、そのデータを使用する際に、そのデータがオリジナル (原本) であるか、未知のソースによって変更されたものであるかについては知る由もない。たとえば、ディスクストレージサブシステムにおいては、権限のない者であってもディスクドライブを取り去り、また、ディスクドライブに保存されている情報を変更し、横取り

50

し、またはコピーすることが可能である。

【0008】

加えて、ストレージシステムに保存されている情報は、長時間経過すると保存しておくには好ましくないものとなってしまうことがある。したがって、ある状況において、古い情報を期限切れにし（たとえばストレージシステムから削除し）、利用できないようにするための方法を準備しておくことが好ましい。このような情報の例としては会社の記録がある。この会社の記録は、会社の方針に従ってたとえば5年後に廃棄される。

【0009】

このように、データを安全に保存・保持する必要性と従来のアプローチの限界に基づけば、特定のデータのコピーが原本であるという比較的高い保証を与えることが可能なデータの保存方法の実現が非常に望まれる。

【0010】

【課題を解決するための手段】

前述した必要性および目的や、以下の説明によって明らかにされる他の必要性および目的は、その一面としてデータの保存方法を含む本発明によって満たされ、かつ実現される。このデータの保存方法は、データをストレージユニットに保存する工程と、そのストレージユニットに許可のないアクセスがあったことを示すタンパ信号（tamper signal）を検知する工程と、タンパ信号を検知した場合に、所定の値をそのデータに上書きすることによって、ストレージユニットに保存されているデータを消去する工程と、を含むものである。

【0011】

本発明の他の面によれば、データを保存するデータストレージユニットが提供される。データストレージユニットは、第1の不揮発性ストレージデバイスと、第1の不揮発性ストレージデバイスに通信できるように接続された処理ユニットとを備え、処理ユニットが、第1の不揮発性ストレージデバイスに対する不正行為があったか否かを判定し、不正行為があったと判定した場合、所定の値をデータに上書きすることによってそのデータを消去するものである。

【0012】

すなわち、請求項1のデータの保存方法は、不揮発性ストレージデバイスにデータを保存するデータストレージユニットのデータの保存方法であって、前記データストレージユニットは、前記データストレージユニットに対する許可のないアクセスを検出するセンサと、前記不揮発性ストレージデバイスおよび前記センサを制御する処理ユニットと、電源に障害が発生した場合に、前記不揮発性ストレージデバイスと、前記センサと、前記処理ユニットとに対して電力を供給可能なバックアップ電源と、を備え、前記処理ユニットは、前記電源に障害が発生した場合に、前記バックアップ電源から前記データストレージユニットへの電力の供給を開始する工程と、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを禁止する工程と、前記センサにより前記データストレージユニットに対するアクセスを検出する工程と、前記データストレージユニットに対するアクセスが検出された場合に、所定の値を前記不揮発性ストレージデバイスに保存されている前記データに上書きすることによって前記不揮発性ストレージデバイスに保存されている前記データを消去する工程と、を含むものである。

【0013】

また、請求項2のデータの保存方法は、請求項1に記載のデータの保存方法において、前記処理ユニットが、さらに、前記電源が回復した後、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを許可する工程を含むものである。

【0014】

また、請求項3のデータストレージユニットは、不揮発性ストレージデバイスにデータを保存するデータストレージユニットであって、前記データストレージユニットに対する

許可のないアクセスを検出するセンサと、前記不揮発性ストレージデバイスおよび前記センサを制御する処理ユニットと、電源に障害が発生した場合に、前記不揮発性ストレージデバイスと、前記センサと、前記処理ユニットとに対して電力を供給可能なバックアップ電源と、を備え、前記処理ユニットは、前記電源に障害が発生した場合に、前記バックアップ電源から前記データストレージユニットへの電力の供給を開始し、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを禁止し、前記センサにより前記データストレージユニットに対するアクセスを検出し、前記データストレージユニットに対するアクセスが検出された場合に、所定の値を前記不揮発性ストレージデバイスに保存されている前記データに上書きすることによって前記不揮発性ストレージデバイスに保存されている前記データを消去するように構成されているものである。

10

【0015】

また、請求項4のデータストレージユニットは、請求項3に記載のデータストレージユニットにおいて、前記処理ユニットは、さらに、前記電源が回復した後、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを許可するように構成されているものである。

【0016】

また、請求項5のコンピュータ読み取り可能な記録媒体は、不揮発性ストレージデバイスにデータを保存するデータストレージユニットに前記データを保存するための一以上の命令の一以上のシーケンスを有するコンピュータ読み取り可能な記録媒体であって、前記データストレージユニットは、前記データストレージユニットに対する許可のないアクセスを検出するセンサと、前記不揮発性ストレージデバイスおよび前記センサを制御する処理ユニットと、電源に障害が発生した場合に、前記不揮発性ストレージデバイスと、前記センサと、前記処理ユニットとに対して電力を供給可能なバックアップ電源と、を備え、前記一以上の命令の一以上のシーケンスは、一以上のプロセッサによって実行される場合に、前記一以上のプロセッサに対し、前記処理ユニットが、前記電源に障害が発生した場合に、前記バックアップ電源から前記データストレージユニットへの電力の供給を開始する手順と、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを禁止する手順と、前記センサにより前記データストレージユニットに対するアクセスを検出する手順と、前記データストレージユニットに対するアクセスが検出された場合に、所定の値を前記不揮発性ストレージデバイスに保存されている前記データに上書きすることによって前記不揮発性ストレージデバイスに保存されている前記データを消去する手順と、を実行させる命令を含むものである。

20

30

【0017】

また、請求項6のコンピュータ読み取り可能な記録媒体は、請求項5に記載のコンピュータ読み取り可能な記録媒体において、前記処理ユニットが、さらに、前記電源が回復した後、前記不揮発性ストレージデバイスへの前記データの書き込みおよび前記不揮発性ストレージデバイスからの前記データの読み出しを許可する手順を実行させる命令を含むものである。

40

【0034】

【発明の実施の形態】

以下においては、あくまでも本発明の説明を目的として特定の具体例を明らかにすることにより、本発明を完全に理解できるようにする。しかし、このような特定の具体例がなくても、本発明が実施可能であることは明らかとなるであろう。なお、いくつかの場合においては、公知の構成および装置をブロック図の形式で示すことにし、発明を不必要に不明瞭にすることを避けることにしている。

【0035】

〔概要〕

ここでは、データを保存して保持すると共に、そのデータにアクセスするためのアプロー

50

チについて説明する。一面において、データはストレージユニットに保存され、所定の時間が経過すると消去される。他の面において、ストレージユニットに対して何らかの不正行為が行われた場合にデータが消去される。さらに他の面において、ストレージユニット内の不揮発性ストレージに何らかの障害が発生した場合にデータが消去される。他のアプローチは、データを永久に保存し、認証することが可能なハードウェアのストレージユニットを含むものである。

【0036】

すなわち、このアプローチは、安全なハードウェアインターフェースおよびソフトウェアインターフェースを有し、それ自身のオペレーティングシステムを備えたデバイスを構築することである。このインターフェースは、データの変更が認められないということを保証する。このように、本発明はデータが本物（原本）であることが重要事項とされる装置において使用することが可能である。以下に、前述した各面について詳細に説明することにする。

【0037】

〔システムの概要〕

図1は、データを保存するためのシステム100を示す図である。図1において、一以上のステーション(station)102は、ネットワーク104を介して互いに接続されている。各ステーション102は、コンピュータ、ワークステーションまたは他の類似の処理機構で構成される。たとえば、各ステーション102は、一実施の形態として図13に示すような種類の汎用コンピュータシステムで構成可能なものである。なお、ステーション102については後に説明する。また、各ステーション102について、クライアント/サーバ環境におけるクライアントに相当すると考えることができる。ネットワーク104を使用することにより、あるステーション102は他の全てのステーション102と通信することが可能となる。

【0038】

また、一以上のストレージユニット106が用意され、データを保存・保持することができるようにしている。このストレージユニット106をリンク108を介してネットワーク104に接続し、ネットワーク104に接続されているステーション102のような他のデバイスと共に動作するようにしても良い。リンク108としては、ストレージユニット106と他のデバイスとの間でデータのやりとりを行うことができるものであればいかなる種類の通信媒体を用いても良い。リンク108の例には、ネットワーク接続、イーサネット・LANもしくはWAN接続、またはあらゆる種類の無線伝送媒体が含まれる。

【0039】

また、リンク108を介してストレージユニット106をネットワーク104に接続することに代え、ストレージユニット106をローカルなリンク112を用いて特定のステーション102に直接接続することにしても良い。また、ストレージユニット106を他の構成で用いることも可能であり、たとえば、ストレージユニット106を特定の数のステーション102に直接接続し、特定のステーション102にローカル・ストレージを提供するようにしても良い。さらに、たとえばSCSIインターフェースのような、ステーションからストレージデバイスへのインターフェースでリンク112を構成することにしても良い。

【0040】

この構成において、各ステーション102は、ネットワーク104を介して適切なメッセージをやり取りすることにより、リンク108を介してストレージユニット106に情報を保存し、またはストレージユニット106から情報を検索して読み出すことが可能となる。

【0041】

また、システム100は、登録オーソリティ(registration authority)110を含んでいる。この登録オーソリティ110は、通信できるようにネットワーク104に接続されていると共に、後に詳細に説明するようにストレージユニット106の登録処理を実行す

る。

【0042】

〔ストレージユニット〕

図2は、ストレージユニット106を示すブロック図である。図2に示すように、ストレージユニット106は、一以上の不揮発性ストレージデバイス200および202を含んでいる。ここでは一実施の形態として二つの不揮発性ストレージデバイス200および202を用意し、データの冗長ストレージを提供することにしている。ただし、本発明は特定の数の不揮発性ストレージデバイス200、202に限定されるものではない（換言すれば、不揮発性ストレージデバイスは、参照符号200および202で示されるように二つに限定されるものではない）。ここでは、図3に示すように、データは不揮発性ストレージデバイス200および202の両方に書き込まれる。

10

【0043】

そのため、図4に示すように、不揮発性ストレージデバイス200および202の一方がたとえば障害の発生によって利用不可能となった場合、データは他方の不揮発性ストレージデバイス200または202に書き込まれる。なお、不揮発性ストレージデバイス200および202としてはいかなる種類のものを用いることにしても良く、その例としては一以上の磁気もしくは光ディスク、テープ、または電源がオフにされた場合であっても保存しているデータを保持可能な他の種類の不揮発性ストレージ等がある。

【0044】

また、ストレージユニット106は、図2にS1～S4として示す一以上のセンサを含み、ストレージユニット106に対する許可のないアクセスを検知することを可能にしている。これらのセンサS1～S4は、たとえばストレージユニット106内への侵入行為、権限なくストレージユニット106にアクセスする行為、または権限なくストレージユニット106をいじったり、使用不能にする行為等を検知するデバイスである。

20

【0045】

具体的に、センサS1～S4は、機械的、電気・機械的または電氣的デバイスであり、検知したイベントに応じて信号（本発明のタンパ信号に該当する）を生成するものである。たとえば、一実施の形態として、各センサS1～S4を、ストレージユニット106のカバーが開けられた際に開きまたは閉じるマイクロスイッチで構成することにしても良い。なお、各センサS1～S4は、リンク208を介して処理ユニット204に接続される。

30

【0046】

また、ストレージユニット106は処理ユニット204を含み、処理ユニット204はリンク108を介してストレージユニット106に対するデータの流れると、ストレージユニット106からのデータの流れるとを制御すると共に、他の処理機能を実行するものである。また、処理ユニット204は、不揮発性ストレージデバイス200および202のオペレーションを制御する。制御するオペレーションには、リンク206を介し、不揮発性ストレージデバイス200および202にデータを書き込むオペレーションや、不揮発性ストレージデバイス200および202からデータを読み出すオペレーションが含まれる。

【0047】

また、処理ユニット204は、センサS1～S4に対し、リンク208を介して通信できるように接続されている。なお、リンク206および208は、リンク108と同様のもので実現可能なものであり、処理ユニット204と不揮発性ストレージデバイス200および202との間でデータのやり取りを可能にすると共に、処理ユニット204とセンサS1～S4との間でデータのやり取りを行うことを可能にしている。

40

【0048】

さらに、ストレージユニット106は、オプションとしてバックアップ電源210および212を含み、ストレージユニット106ならびにその構成要素、すなわち不揮発性ストレージデバイス200・202、処理ユニット204およびセンサS1～S4等に電力を供給できるようにしている。理論的には、バックアップ電源210および212が実装されることによって、電力不足の場合にバックアップ電源210および212のいずれか一

50

方がストレージユニット 106 の動作に十分な電力を供給することができる。

【0049】

たとえば、バックアップ電源 210 および 212 をバッテリまたは無停電電源 (uninterruptible power supply; UPS) を使用することによって実現することにしても良い。なお、バックアップ電源 210 および 212 の一方を、処理ユニット 204 に対してバックアップ電力を供給するオンボード・バッテリ (onboard battery) とすることが好ましい。

【0050】

〔処理ユニット〕

図 5 は、処理ユニット 204 を示すブロック図である。処理ユニット 204 は、通信インターフェース 300 を含んでいる。この通信インターフェース 300 は、リンク 108 を介して処理ユニット 204 とストレージユニット 106 外部の他のデバイスとの間の通信を制御し、バッファリングし、かつ規制する。なお、この通信インターフェース 300 としては、たとえば、SCSI, IEEE1394 またはイーサネットコントローラのような I/O コントローラを用いることができる。

10

【0051】

また、処理ユニット 204 はセンサコントローラ 302 を含んでいる。このセンサコントローラ 302 は、リンク 208 を介し、センサ S1 ~ S4 と処理ユニット 204 との間のインターフェースとなり、センサ S1 ~ S4 と処理ユニット 204 との間で通信を行えるようにする。なお、センサコントローラ 302 としては、たとえばアナログ I/O インターフェースを用いることができる。

20

【0052】

また、処理ユニット 204 は、リンク 206 を介して不揮発性ストレージデバイス 200 および 202 を制御する不揮発性ストレージコントローラ 304 を含んでいる。この不揮発性ストレージコントローラ 304 は、たとえばディスクコントローラである。また、処理ユニット 204 は、処理ユニット 204 およびここで説明されるその構成要素の動作を制御するプロセッサ 306 を含んでいる。このプロセッサ 306 は、たとえばマイクロプロセッサである。

【0053】

さらに、処理ユニット 204 は、RAM のような揮発性メモリ 308 を含んでおり、揮発性メモリ 308 はデータやプロセッサ 306 の命令を記憶するものである。また、処理ユニット 204 は、たとえば ROM, PROM, EPROM, フラッシュメモリまたは他の種類のメモリ等のような不揮発性メモリ 310 を含んでいる。

30

【0054】

通信インターフェース 300, センサコントローラ 302, 不揮発性ストレージコントローラ 304, プロセッサ 306, 揮発性メモリ 308 および不揮発性メモリ 310 は、それぞれリンク 312 を介して通信できるように接続されており、これによってこれらの構成要素間で通信を行えるように構成されている。リンク 312 の例としては、通信バス、またはアドレスバスおよびデータバスの組み合わせが挙げられる。

【0055】

なお、処理ユニット 204 は、UNIX のようなリアルタイムオペレーティングシステム (OS) の制御の下で動作するものであることが好ましい。記憶されている一以上のプログラムは OS の下で動作し、ここでさらに説明するストレージユニット 106 のオペレーションおよびプロセスを管理する。

40

【0056】

〔不揮発性ストレージ〕

図 6 は、不揮発性ストレージデバイス 200 および 202 の内容を示す図である。各不揮発性ストレージデバイス 200 および 202 は、ストレージ ID 情報 400 を含みまたは保存している。このストレージ ID 情報 400 は、不揮発性ストレージデバイス 200 および 202 をユニークに (一意に) 識別するためのものである。たとえば、ストレージ ID 情報 400 は、不揮発性ストレージデバイス 200 および 202 のユニークなシリアル

50

ナンバーを含むものであっても良い。また、ストレージID情報400は、ストレージユニット106の登録処理の間に得られた情報、すなわちストレージユニット106を認証するために使用される情報を指定する。なお、ストレージユニット106を登録する処理については後に詳細に説明することにする。

【0057】

また、不揮発性ストレージデバイス200および202はディレクトリ情報402を含んでいる。このディレクトリ情報402は、不揮発性ストレージデバイス200および202上に保存されているデータ404に関する情報を指定するものである。一実施の形態によれば、データ404は複数のデータファイルを含んでおり、また、ディレクトリ情報402はデータ404のデータファイルに関する情報に対応し、かつその情報を指定する複数のディレクトリエントリ500を含んでいる。ファイル指向のストレージシステムは不要である。データ404はあらゆる種類の保存された情報であって良く、また、ディレクトリ情報402はデータ404について記述するものであればどのようなメタデータであってても良い。

【0058】

図9は、一実施の形態におけるディレクトリエントリ500の内容を示す図である。ディレクトリエントリ500は、対応するデータファイルの名称（ファイル名（File Name）502）、対応するデータファイルの作成日付（作成日付（Creation Date）504）、対応するデータファイルの有効期限が満了する日付（有効期限（Expiration Date）506）および特定のアプリケーションに応じて変更可能な他のファイル管理情報508を示すものである。なお、他のファイル管理情報は、たとえば、アプリケーション等に関連するファイルの種類である。

【0059】

また、ディレクトリエントリ500は複製情報（replication information）510の記述を含んでいる。複製情報510は、一以上のディレクトリエントリ512（R1, R2, ..., RN）を示すことにより、ファイル名502のファイルに関連するデータファイルのソースを示している。各ディレクトリエントリ512は、ストレージID情報、複製日付、およびストレージIDのディレクトリパスによる親データの完全な履歴を含んでいる。なお、データのファイル名502はオリジナル（原本）から変更されることはなく、また、有効期限506のデータもコピーされる。

【0060】

なお、「有効期限」は、ここで使用されているように、関連するデータが無効または使用不可能とされる時間、日または日付を意味する。不揮発性ストレージデバイス200、202中の情報はOSによって管理される。

【0061】

〔有効期限満了後の消去〕

一実施の形態において、不揮発性ストレージデバイス200および202に保存されているデータは、特定の期間が経過すると消去される。このプロセスは、特定のデータを対象として実行されるものであり、このことは異なるデータは異なる期間にわたって不揮発性ストレージデバイス200および202上に存在していても良いということを意味している。また、異なるデータ毎に異なる有効期限を適用することにしても良い。さらに、一部のデータについては消去されないようにしても良く、すなわち無期限に不揮発性ストレージデバイス200および202上に存在するようにしても良い。

【0062】

図6、図9および図10において、ディレクトリ情報402に含まれているディレクトリエントリ500は、有効期限506が満了するに至ったか否かを判定するために調査される。この処理は、特定のディレクトリエントリ500の有効期限506と現在の日付とを比較することによって実行される。また、各ディレクトリエントリ500に有効期限506を保持させておくことに代え、各ディレクトリエントリ500に「保持期間（“time to keep”）」を保持させるようにし、作成日付504および「保持期間」の両方に基づい

て有効期限を決定することにしても良い。また、代替的なアプローチは、全てのディレクトリの全てのエントリを巡回し、エントリの有効期限とシステムの時間および日付とをチェックするエージェントを持つことである。有効期限が経過している場合、エージェントは該当するエントリを削除する。

【0063】

図10は、データを消去するための好適な方法を示すフローチャートである。ステップS520において、現在の日付／時間値が取得される。たとえば、処理ユニット204は、処理ユニット204のオペレーションを制御する、オペレーティングシステムの機能をコールすることによって日付／時間値を要求し、それを取得する。これに代えて、プロセス306が直接問い合わせることが可能なクロックを処理ユニット204に含めることにしても良い。なお、現在の日付／時間値は、図10に示す方法を実行する現在の日、日付または時間を示すものである。また、現在の日付／時間値をCPUレジスタ、作業用記憶領域（scratchpad memory area）またはメインメモリのような一時的な記憶場所に記憶し、後で使用できるようにすることが好ましい。

【0064】

続いて、ステップS522において、一つのディレクトリエントリ500が選択され、処理される。一実施の形態において、ステップS522は不揮発性ストレージデバイス200、202中の全てのディレクトリエントリ500をシリアルにポーリングする処理（serial polling）を含む。また、ステップS522が、たとえばLRU法（least-recently-used）アルゴリズム、確率または統計のようなヒューリスティック・プロセス（heuristic process）に基づいてディレクトリエントリ500を選択する処理を含むようにしても良い。

【0065】

そして、ステップS524において、カレントのディレクトリエントリ（current directory entry）500によって表されるデータを消去するか否かが決定される。一実施の形態において、ステップS524は、ステップS520で取得した現在の日付／時間値がカレントのディレクトリエントリ500中に保存されている有効期限506の値以上であるか否かをテストする処理を含む。現在の日付／時間値が有効期限506の値以上である場合、そのカレントのディレクトリエントリ500は消去されることになる。

【0066】

特定のデータを消去すると判定されると、ステップS526に示すように、データ404からカレントのディレクトリエントリ500に関連するデータが消去される。そして、制御はステップS534に進む。その特定のデータが消去されると、ステップS534に示すように、ディレクトリエントリ500も消去される。なお、消去された特定のデータのコピーは同一の有効期限を含んでおり、かつその有効期限がチェックされることから、その特定のデータの全てのコピーもデータ404から消去されることになる。

【0067】

なお、一実施の形態によれば、ステップS526およびS534において、データ404からデータを消去すると共に、対応するディレクトリエントリ500をディレクトリ情報402から消去する処理は、所定の値をそのデータおよびディレクトリエントリ500に上書きすることによって実行される。適当と認められる所定の値の例は00Hであるが、所定の値として他の値を使用することにしても良い。

【0068】

ある従来のアプローチは、データそのものを消去することなく単にディレクトリエントリを消去するだけであったことから、消去したデータを回復させることが可能であった。これに対し、データが上書きされるとその回復はより困難なものとなるため、所定の値をデータに上書きすることによってより確実にそのデータを消去したものと考えられる。所定の値を上書きすることによって、データがデータ404から消去されると共に、対応するディレクトリエントリ500がディレクトリ情報402から消去されると、上書きされた領域は他のデータを保存するために使用されることになる。

【0069】

代替的な実施の形態においては、異なるデータ毎に異なる所定の値を用いて上書きが行われる。たとえば、不揮発性ストレージデバイス200上に存在している特定のデータファイルの有効期限506が、その特定のデータファイルが削除されるものであることを示しているものとする。また、その特定のデータファイルのコピーが、不揮発性ストレージデバイス202上に保持されているものとする。この場合において、不揮発性ストレージデバイス200上の特定のデータファイルには第1の所定の値が上書きされ、一方、不揮発性ストレージデバイス202上のその特定のデータファイルのコピーには第1の所定の値と異なる第2の所定の値が上書きされる。また、対応するディレクトリエントリ500に上書きするために、異なる所定の値を用いることにしても良い。

10

【0070】

一実施の形態において、図10のプロセスは処理ユニット204によって実行される。特に、プロセッサ306が、揮発性メモリ308および不揮発性メモリ310に保持されている一以上の命令を実行することによってこのプロセスを実行することにしても良い。これに対し、ストレージユニット106の外部の別のプロセスまたはネットワーク104に接続されているステーション102等により、ディレクトリ情報402中の各ディレクトリエントリ500を調査するプロセスを実行することにしても良い。このような場合において、他のプロセスまたはステーション102は、リンク108を通してストレージユニット106に問合せし、ディレクトリ情報402を取得することにしても良い。

20

【0071】

以上では、ストレージID情報400、ディレクトリ情報402およびデータ404が、不揮発性ストレージデバイス200および202上で一緒に保持されるものとして説明・図示することにしたが、これらの情報の一部を他とは別に他の記憶位置に保持させることにしても良い。たとえばディレクトリ情報402の一部または全てを処理ユニット204の揮発性メモリ308に保持しておくことにしても良く、これによりデータ404から削除する必要があるデータファイルを判定するために必要な時間を短縮することが可能となる。

【0072】

〔不揮発性ストレージデバイスに障害が発生した後の消去〕

別の実施の形態によれば、不揮発性ストレージデバイス200および202の一方に何らかの障害が発生した場合、データ404に含まれる全てのデータおよびディレクトリ情報402に含まれる全てのディレクトリエントリ500が前述したように消去される。そして、他方の不揮発性ストレージデバイス200または202が第1のストレージデバイス(primary storage device)として指定され、継続して使用される。

30

【0073】

障害が発生するような状況の一例は、両方の不揮発性ストレージデバイス200および202のアップデートが行われている際に、メディアの破損が不揮発性ストレージデバイス200および202の一方のアップデートを妨げるような場合である。不揮発性ストレージデバイス200および202が冗長ストレージを提供することから、障害が発生した不揮発性ストレージデバイス200または202からデータを削除することにより、不揮発性ストレージデバイス200および202が異なる(およびおそらく有効な)データを含まないようにする。

40

【0074】

図11は、不揮発性ストレージデバイスに何らかの障害が発生した場合に、その不揮発性ストレージデバイスのデータを消去するための好適な方法を示すフローチャートである。ステップS540において、不揮発性ストレージデバイスに何らかの障害が発生していることが検知される。たとえば、ステップS540が、パワーアップ・ルーチン(power-up routine)またはブートストラップ・ローダ・ルーチン(bootstrap loader routine)において電源異常または他の障害が生じていることを検知するステップを含むようにしても良い。

50

【0075】

一実施の形態において、各不揮発性ストレージデバイス200, 202は、マーカ値 (marker value) を保存する専用の記憶場所を持つ。このマーカ値は、不揮発性ストレージデバイス200, 202が問題なくシャットダウンされたことを示す予め定められた値である。不揮発性ストレージデバイス200, 202が問題なくシャットダウンされる場合に、予め定められたマーカ値が専用の記憶場所に保存される。

【0076】

一方、不揮発性ストレージデバイス200, 202が起動される場合に、予め定められたマーカ値がチェックされ、そして異なる値が上書きされる。したがって、予想外の障害 (たとえば異常終了) が起こると、専用の記憶場所にはマーカ値が含まれていないことになり、それによって不揮発性ストレージデバイス200, 202に障害が発生したことが検知される。

10

【0077】

ある障害の発生が検知された場合、ステップS542において複数のディレクトリエントリ500の中から次のディレクトリエントリ500が選択される。一実施の形態において、ステップS542は、不揮発性ストレージデバイス200, 202中の全てのディレクトリエントリ500をシリアルにポーリングするステップを含んでいる。また、ステップS542は、LRU法 (least-recently-used) アルゴリズム、確率または統計のようなヒューリスティック・プロセス (heuristic process) に基づいてディレクトリエントリ500を選択するステップを含むようにしても良い。

20

【0078】

そして、ステップS544において、カレントのディレクトリエントリ500と関連付けられるデータの全てが、たとえば所定の値をそれらのデータに上書きすることによって消去される。そして、ステップS552において、カレントのディレクトリエントリ500は、たとえばそれに所定の値を上書きすることによって消去される。必要な場合、ディレクトリそのものも消去される。

【0079】

続いて、ステップS554において、さらなるディレクトリエントリ500が不揮発性ストレージデバイス200, 202のディレクトリ情報402中に存在するか否かが判定される。存在すると判定された場合、ステップS542～S552が、さらなるディレクトリエントリ500それぞれ対して繰返し実行される。

30

【0080】

任意のステップS556において、他の不揮発性ストレージデバイス200または202がストレージユニット106の第1の (primary) ストレージデバイスとして指定される。このような指定は、ストレージユニット106が障害のない不揮発性ストレージデバイス200または202を対象として読み出し／書き込みオペレーションを継続することであることを意味する。このように、ストレージユニット106は使用可能なままであるが、ストレージユニット106内の障害が発生した不揮発性ストレージデバイス200または202は使用不可能とされる。

【0081】

40

障害が発生した不揮発性ストレージデバイス200または202のデータが消去されると、障害が発生した不揮発性ストレージデバイス200または202を再初期化するようにしても良い。障害が発生した不揮発性ストレージデバイス200または202がうまく再初期化されると、障害が発生しなかった不揮発性ストレージデバイス200または202に保存されているデータを回復した不揮発性ストレージデバイス200または202にコピーすることができる。障害が発生した不揮発性ストレージデバイス200または202をうまく再初期化することができなかった場合、障害が発生しなかった不揮発性ストレージデバイス200または202のデータを別のストレージユニット106の不揮発性ストレージデバイスにコピーすることにしても良い。

【0082】

50

不揮発性ストレージデバイス 200 および 202 に同時に障害が発生する可能性は非常に低い、冗長不揮発性ストレージデバイス 200, 202 を使用することにより、非常に高いデータの信頼性を提供することができる。さらなるデータの信頼性を提供するため、冗長不揮発性ストレージデバイス 200 および 202 をそれぞれ含む他の複数のストレージユニット 106 を使用して、さらなる冗長性を提供することもできる。

【0083】

〔不正の防止 (tamper protection) 〕

一実施の形態によれば、ストレージユニット 106 は不正行為から保護される。センサ S1～S4 は、リンク 208 を通して処理ユニット 204 によって監視されており、ストレージユニット 106 に対する不正行為を検知する。センサ S1～S4 の選択および配置については特定のアプリケーションの要件によって決定されるものではあるが、一般に、シールを破壊すること、密封された仕切りを開くこと、その他、ストレージユニット 106 に力づくで侵入すること等を通じてストレージユニット 106 に対する許可のないアクセスを検知するように設計される。

10

【0084】

センサ S1～S4 がストレージユニット 106 に対する許可のないアクセスを検知した場合、センサ S1～S4 はタンパ信号 (tamper signal ; すなわち、ストレージユニット 106 に対する不正を検知したことを示す信号) を処理ユニット 204 に入力する。処理ユニット 204 は、タンパ信号に応じて、前述した方法で不揮発性ストレージデバイス 200 および 202 からストレージ ID 情報 400, ディレクトリ情報 402 およびデータ 404 を消去する。これにより、ストレージユニット 106 に保存されているデータが許可なく使用されることが防止される。

20

【0085】

図 12 は、ストレージユニット 106 に不正行為が行われた場合に、不揮発性ストレージデバイス 200 および 202 の記憶内容を消去する好適な方法を示すフローチャートである。ステップ S560 において、たとえばストレージユニット 106 に不正を働くこと、ストレージユニット 106 に侵入すること、ストレージユニット 106 を空けること等のようなストレージユニット 106 に対する外乱が検知される。たとえば、ステップ S560 が、一以上のセンサ S1～S4 が作動され、または検知信号を生成していることを検知するステップを含むことにしても良い。

30

【0086】

不正行為が検出された場合、ステップ S562 において、複数のディレクトリエントリ 500 の中からつぎのディレクトリエントリ 500 が選択される。一実施の形態において、ステップ S562 は不揮発性ストレージデバイス 200, 202 の全てのディレクトリエントリ 500 に対してシリアルにポーリングするステップを含む。また、ステップ S562 は、たとえば LRU 法 (least-recently-used) アルゴリズム、確率または統計のようなヒューリスティック・プロセスに基づいてディレクトリエントリを選択するステップを含むものであっても良い。

【0087】

続いて、ステップ S564 において、カレントのディレクトリエントリ 500 に関連する全てのデータは、たとえば所定の値をそれらのデータに上書きすることによって消去される。また、ステップ S572 において、カレントのディレクトリエントリ 500 は、たとえば所定の値をそれに上書きすることによって消去される。また、必要な場合には、ディレクトリそのものも消去される。

40

【0088】

そして、ステップ S574 において、さらなるディレクトリエントリ 500 が不揮発性ストレージデバイス 200, 202 のディレクトリ情報 402 に存在するか否かが判定される。さらなるディレクトリエントリ 500 が存在すると判定された場合、各ディレクトリエントリ 500 についてステップ S562～S572 までの処理が繰り返し実行される。

【0089】

50

一実施の形態において、ステップ S 5 6 2 または他のステップが、権限を有する者に対する警告を生成して、不正行為が発生し、消去のオペレーションが実行されたことを知らせるステップを含むようにしても良い。たとえば、ステップ S 5 6 2 において、処理ユニット 2 0 4 は所定のステーション 1 0 2 に対するメッセージを生成し、不正行為が検出され、消去オペレーションが進行中であることをそのステーション 1 0 2 に通知することにしても良い。

【0090】

別の実施の形態によれば、電源異常（たとえば停電）の場合に、バックアップ電源 2 1 0 および 2 1 2 は、センサ S 1 ～ S 4 を含むストレージユニット 1 0 6 に電力を供給する。ところが、不揮発性ストレージデバイス 2 0 0 および 2 0 2 は、パワーセーブモードで動作する。パワーセーブモードで動作する場合、不揮発性ストレージデバイス 2 0 0 および 2 0 2 に対する通常の書き込みおよび読み出しオペレーションは電力を節約するために禁止される。電源が回復すると、不揮発性ストレージデバイス 2 0 0 および 2 0 2 に対する書き込みおよび読み出しオペレーションが続けられることになる。

【0091】

ただし、ストレージユニット 1 0 6 がパワーセーブモードで動作している間であろうとも、センサ S 1 ～ S 4 がストレージユニット 1 0 6 に対する許可のないアクセスを検出した場合にあっては、利用可能な全ての電力を利用して前述したように不揮発性ストレージデバイス 2 0 0 および 2 0 2 からストレージ ID 情報 4 0 0、ディレクトリ情報 4 0 2 およびデータ 4 0 4 が消去される。このように、単にストレージユニット 1 0 6 の電源を切る

【0092】

〔ストレージユニットの登録〕

一実施の形態によれば、ストレージユニット 1 0 6 は、ストレージユニット 1 0 6 の認証を行うために登録オーソリティ 1 1 0 に登録される。このアプローチによると、各ストレージユニット 1 0 6 は、登録オーソリティ 1 1 0 にユニークなストレージユニット識別子値を与えることによって登録オーソリティ 1 1 0 に登録される。これに応じて、登録識別子値が登録オーソリティ 1 1 0 によって与えられ、不揮発性ストレージデバイス 2 0 0 および 2 0 2 のストレージ ID 情報 4 0 0 中に保存される。

【0093】

このようにしてストレージユニット 1 0 6 が登録されると、ステーション 1 0 2 は、特定のストレージユニット 1 0 6 の登録識別子値をリクエストし、そして登録オーソリティ 1 1 0 で登録識別子値が有効であることを確認することにより、特定のストレージユニット 1 0 6 が登録オーソリティ 1 1 0 に登録されていることを確認することができる。これにより、特定のストレージユニット 1 0 6 に保存されているデータがオリジナル（原作）で真性であることが保証される。

【0094】

図 7 は、ヘッダ・セグメント 4 2 2、デバイス・メーカー・セグメント 4 2 4 およびシリアル・ナンバー・セグメント 4 2 6 を有する登録識別子値 4 2 0 の好適な例を示す図である。

【0095】

ヘッダ・セグメント 4 2 2 は、登録オーソリティ 1 1 0 を特定するものである。たとえば、ヘッダ・セグメント 4 2 2 は、ストレージユニット 1 0 6 または OS のコンテキスト内において、登録オーソリティ 1 1 0 と一意的に関連付けられる所定の値を含む。デバイス・メーカー・セグメント 4 2 4 は、一意的にストレージユニット 1 0 6 のメーカまたはブランド名を特定するものである。このデバイス・メーカー・セグメント 4 2 4 は、特定のメーカを一意に特定するメーカ名またはコード番号であっても良い。また、シリアル・ナンバー・セグメント 4 2 6 は、ストレージユニット 1 0 6 のシリアル・ナンバーを含むものである。

【0096】

図8は、データベース111の説明図である。データベース111は、一以上の行462を有する少なくとも一つのテーブル460を備えている。各行462は一つのストレージユニット106に対応する。テーブル460は、メーカーまたはブランド名の値、シリアルナンバー値および割当て日付の値を格納する列464～468を有している。各割当て日付の値は、あるストレージユニット106に相当する行がテーブル460に加えられた日付けを特定するものである。

【0097】

〔データのオリジナリティ〕

ある状況においては、あるデータを変更しないようにし、または削除しないようにすることによって、ストレージユニット106に保存されているそのあるデータのオリジナリティおよびユニークさを保つようにすることが好ましい場合がある。このようにすることにより、ストレージユニット106は、あるデータが最初に書き込まれた時から変更されていないことを外部のプロセスまたはデバイスに「保証する (guarantee) 」ことができる。

10

【0098】

一実施の形態においては、あるデバイスから別のデバイスにデータをコピーする場合に、追跡記録 (audit trail) が生成される。図9に示すように、各複製エントリ (R1, R2, …, RN) は、複製日付514ならびにストレージID情報516およびディレクトリエントリ512を含むソース情報を記述するものである。ソース (source) ・デバイスからディスティネーション (destination) ・デバイスへデータを複製するために、ファイル情報やソース・デバイスのスペックと共に、複製コマンドがディスティネーション・デバイスに対して発行される。

20

【0099】

そして、ディスティネーション・デバイスはソース・デバイスに対して特別な読出コマンドを発行し、ソース・デバイスからディスティネーション・デバイスに転送される際にデータが変更されてしまうことを避けることができるように、そのデータが暗号化される。

【0100】

したがって、一実施の形態によれば、ストレージユニット106に保存されているあるデータは一度だけ書き込まれ、決して変更されていないことを保証するためのアプローチが提供されることになるが、そのあるデータが読み出し専用 (read-only) として無制限の回数読み出しできるものであっても良い。このアプローチは特定のデータを対象とするものであって、保存されている全てのデータを読み出し専用データとして保持することを要求するものではない。

30

【0101】

一実施の形態においては、読み出し専用データが不揮発性ストレージデバイス200および202に保存された後、読み出し専用データに関連するディレクトリエントリ500がアップデートされ、関連するデータが読み出し専用データであり、かつ、決して上書きまたは変更されることがないものであることが示される。このアップデートは、保存されているデータがユニーク (固有) かつ、不変なものであることを他のデバイスやプロセスに宣言するというように作用する。たとえば、読み出し専用データが不揮発性ストレージデバイス200および202に書き込まれた後、読み出し専用データと関連付けられるディレクトリエントリ500の他のファイル管理情報508は、関連付けられたデータが読み出し専用であって変更されることがないということを表すように更新される。

40

【0102】

その後、不揮発性ストレージデバイス200および202のデータが変更されることになる場合、そのデータと関連付けられているディレクトリエントリ500が調査され、その特定のデータが読み出し専用であるか否かが判定される。読み出し専用ではない場合、関連付けられているデータはここで説明されるように変更される。一方、読み出し専用である場合、関連付けられているデータおよびディレクトリエントリ500は変更されることはない。

50

【0103】

オリジナリティを保証する別の方法としては、特定の不揮発性ストレージデバイス上で実行可能な書込みコマンドを制限するというものがある。たとえば、不揮発性ストレージデバイスに保存されているファイルがオリジナリティを保証するために認証されたファイルであるとして保持されている状況に関連して、その不揮発性ストレージデバイスが書き込みのための特別なステータスを要求することにしても良い。特別な書き込みステータスがないと、同一ファイル名が不揮発性ストレージデバイスに存在する場合に書き込みコマンドは失敗に終わることになる。

【0104】

このアプローチは、有効期限に基づく消去処理、不正行為に基づく消去処理および障害の発生に基づく消去処理を含む、ここで説明されるあらゆるアプローチに適用することができるものである。このアプローチは、保存されているデータの有効性を保証する方法を提供し、その結果、保存されているデータの信頼性の向上、たとえば法的な証拠としてのデータの信頼性の向上が図られる。また、データの内容およびユニークさも保証される。

【0105】

〔コンピュータシステムの概要〕

図13は、本発明の各面を実現するために使用可能なコンピュータシステムを示すブロック図であり、たとえば、処理ユニット204の代替的な実施の形態を示すものである。処理ユニット204は情報通信のためにバス602または他の通信機構を含み、プロセッサ604は情報を処理するためにバス602と接続されている。また、処理ユニット204は、たとえばランダムアクセスメモリ（RAM）または他の動的ストレージデバイスのようなメインメモリ606を含み、メインメモリ606は、情報やプロセッサ604によって実行される命令を保存するためにバス602に接続されている。

【0106】

また、メインメモリ606を使用して、プロセッサ604によって実行される命令の実行中に一時変数または他の中間情報を格納することにしても良い。さらに、処理ユニット204は、静的な情報やプロセッサ604に対する命令を記憶するためにバス602に接続されたリードオンリーメモリ（ROM）608または他の静的なストレージデバイスを含んでいる。また、ストレージデバイス610は、たとえば磁気ディスクや光ディスクであり、バス602に接続されて情報および命令を記憶できるようになっている。

【0107】

また、処理ユニット204を、たとえばCRTのようなコンピュータのユーザに情報を表示するためのディスプレイ612にバス602を通して接続するようにしても良い。英数字および他のキーを含む入力デバイス614は、バス602に接続されてプロセッサ604に情報およびコマンド選択を送信できるようになっている。別の種類のユーザ入力装置は、マウス、トラックボールまたはカーソル方向キーのようなカーソルコントロール616であり、これは方向の情報やコマンド選択をプロセッサ604に送信すると共に、ディスプレイ612上のカーソルの動きを制御する。このような入力装置は、一般に、第1の軸（たとえばx）および第2の軸（たとえばy）という二つの軸において2つの自由度を持つことにより、平面における位置を指定することを可能にしたものである。

【0108】

本発明はストレージユニット106を使用してデータを保存する技術に関連するものである。一実施の形態においては、メインメモリ606に保存されている一以上の命令の一以上のシーケンスをプロセッサ604が実行することに応じて、処理ユニット204によってデータを保存し、保持する処理が実行される。このような命令は、ストレージデバイス610のような別のコンピュータ読み取り可能な媒体からメインメモリ606に読み込まれるものであっても良い。メインメモリ606に含まれる命令のシーケンスを実行することにより、プロセッサ604はここで説明したプロセスの各ステップを実行する。

【0109】

また、マルチプロセッシング構成における一以上のプロセッサを使用して、メインメモリ

10

20

30

40

50

606に含まれる命令のシーケンスを実行することにしても良い。代替的な実施の形態として、ハードワイヤード回路をソフトウェア命令の代わりに、またはソフトウェア命令と組み合わせて使用することにより、本発明を実現することも可能である。したがって、本発明の各実施の形態はハードウェアおよびソフトウェアの特定の組み合わせに限定されるものではない。また、命令は、ソフトウェアエージェント、プロセス、サブルーチンまたはプログラムとして構成可能である。

【0110】

ここで使用される「コンピュータ読み取り可能な媒体」という用語は、プロセッサ604に命令を与えて実行させることに関与するあらゆる媒体を指す。このような媒体は、不揮発性媒体、揮発性媒体および伝送媒体を含む多くの形態を取ることが可能なものである。ただし、このような形態に限定されるものではない。たとえば、不揮発性媒体は、ストレージデバイス610のような光または磁気ディスクを含むものである。

10

【0111】

また、揮発性媒体は、メインメモリ606のようなダイナミックメモリを含むものである。さらに、伝送媒体は、同軸ケーブル、銅線および光ファイバを含むものであり、バス602を構成するワイヤを含むものである。なお、伝送媒体は、電波および赤外線通信時に生成されるような音波または光波のような形態をとることができる。

【0112】

また、コンピュータ読み取り可能な媒体の一般的な形態には、たとえば、フロッピーディスク、フレキシブルディスク、ハードディスク、磁気テープもしくは他の磁気媒体、CD-ROMや他のあらゆる光学媒体、パンチカード、紙テープもしくは穴によるパターンを有する他のあらゆる物理的な媒体、RAM、PROMおよびEPROM、FLASH-EPROM、他のあらゆるメモリチップもしくはカートリッジ、後述する搬送波、またはコンピュータが読み出し処理を行うことが可能な他のあらゆる媒体が含まれる。

20

【0113】

様々な形式のコンピュータ読み取り可能な媒体が、プロセッサ604で実行するための一以上の命令の一以上のシーケンスを保持するために必要とされる。たとえば、リモートコンピュータの磁気ディスク上に最初に命令が保持されることにしても良い。リモートコンピュータは、命令をそのダイナミックメモリにロードし、モデムを使用することにより電話回線を介して命令を送信することができる。処理ユニット204内部のモデムは電話回線を介してデータを受信し、赤外線送信機を使用してデータを赤外線信号に変換することができる。

30

【0114】

バス602に接続されている赤外線検出器は、赤外線信号で運ばれているデータを受信し、バス602に送出することができる。バス602はデータをメインメモリ606に運び、プロセッサ604はそこから命令を読み出して実行する。メインメモリ606で受信された命令を、プロセッサ604による実行の前か後にストレージデバイス610にオプションとして保存するようにしても良い。

【0115】

また、処理ユニット204は、バス602に接続された通信インターフェース618を含んでいる。通信インターフェース618は、ローカルネットワーク622に接続されているネットワークリンク620に対し、双方向データ通信カップリングを提供する。たとえば、通信インターフェース618をISDN(Integrated Services Digital Network)カードまたはモデムで構成することにし、対応する種類の電話回線に対してデータ通信接続を提供するようにしても良い。

40

【0116】

別の例として、通信インターフェース618をローカルエリアネットワーク(LAN)カードで構成することにし、互換LANにデータ通信接続を提供するようにしても良い。また、無線リンクを実装することにしても良い。どのようなインプリメンテーションにおいても、通信インターフェース618は、様々な種類の情報を表すデジタルデータのスト

50

リームを伝送する電氣的，電気磁氣的または光学的信号を送信し、かつ受信する。

【0117】

ネットワークリンク620は、概して、データ通信を一以上のネットワークを介して他のデータデバイスに提供するものである。たとえば、ネットワークリンク620は、ローカルネットワーク622を介してホストコンピュータ624またはインターネットサービスプロバイダ（ISP）626によって管理されているデータ機器に対する接続を提供する。ISP626は、現在一般に「インターネット」628と呼ばれる世界的なパケットデータ通信網を介してデータ通信サービスを提供するものである。

【0118】

ローカルネットワーク622およびインターネット628の両方とも、電気信号，電気磁気信号または光信号を使用してデジタルデータのストリームを搬送するものである。様々なネットワークを経る信号，ならびにネットワークリンク620上および通信インタフェース618を経る信号は、処理ユニット204にデジタルデータを搬送し、または処理ユニット204からデジタルデータを搬送するものであり、情報を搬送する搬送波に関する例示的な形態である。

【0119】

処理ユニット204は、一以上のネットワーク，ネットワークリンク620および通信インタフェース618を通して、プログラムコードを含むメッセージを送信し、かつプログラムコードを含むデータを受信することができる。インターネットの例において、サーバ630は、インターネット628，ISP626，ローカルネットワーク622および通信インタフェース618を通して、リクエストされたアプリケーションプログラムのコードを伝送することも可能である。このようにダウンロードされたアプリケーションは、ここで説明したようにデータを保存し、保持する処理を実行する。

【0120】

データが受信された場合および／または後に実行するためにストレージデバイス610もしくは他の不揮発性ストレージに保存された場合に、受信されたコードがプロセッサ604によって実行されるようにしても良い。このように、処理ユニット204は、搬送波の形態でアプリケーションコードを取得するものであっても良い。

【0121】

ここで記述される手法は、データを保存して保持することに関し、従来のアプローチを越えるいくつかの利点を与えるものである。特に、所定の値をデータに上書きすることでストレージユニット106からそのデータを消去するアプローチを採用することにより、そのデータの回復をより困難なものとする。不正行為を監視することにより、許可されていないアクセスからストレージユニット106を保護する。登録オーソリティ110を使用してストレージユニット106を登録することにより、ストレージユニット106に保存されているデータを認証する。

【0122】

さらに、データのオリジナリティを保つためのアプローチは、あるデータがストレージユニット106から読み出される場合にそのあるデータが一度だけ書き込まれたものであり、かつ変更が加えられたものではないことを保証する。同様に、データがストレージユニット106から消去される際に、読み出し専用データとして指定されているデータはストレージユニット106から消去されることはない。

【0123】

〔変形例〕

以上のように、ある特定の実施の形態に基づいて本発明を説明した。しかし、本発明のより広い精神および範囲から逸脱することなく、本発明に対して様々な設計変更を行うことが可能なことは明らかである。したがって、明細書および図面は、あくまでも例示としてみなされるものであって、本発明を限定することを意図するものではない。

【0124】

【発明の効果】

10

20

30

40

50

以上説明したように、本発明のデータの保存方法、データストレージユニットおよびコンピュータ読み取り可能な記録媒体によれば、少なくとも、不正行為からデータを保護することができるという効果を得ることができる。

【図面の簡単な説明】

【図１】データを保存・保持するシステムを示すブロック図である。

【図２】図１のシステムに含まれるストレージユニットを示すブロック図である。

【図３】図２のストレージユニットの一部を示すブロック図である。

【図４】図２のストレージユニットの一部を示すブロック図である。

【図５】図２～図４のストレージユニットに含まれる処理ユニットを示すブロック図である。

10

【図６】図２～図４のストレージユニットに含まれる不揮発性ストレージデバイスの内容を示すブロック図である。

【図７】登録識別子値を示す説明図である。

【図８】登録オーソリティのデータベースのテーブルを示す説明図である。

【図９】図６の不揮発性ストレージデバイスに含まれるディレクトリエントリの内容を示す説明図である。

【図１０】有効期限に基づく消去プロセスを示すフローチャートである。

【図１１】障害の発生に基づく消去プロセスを示すフローチャートである。

【図１２】不正行為に基づく消去プロセスを示すフローチャートである。

【図１３】本発明の実施の形態を実現可能なコンピュータシステムのブロック図である。

20

【符号の説明】

- １００ システム
- １０２ ステーション
- １０４ ネットワーク
- １０６ ストレージユニット
- １０８，１１２，２０６，２０８，３１２ リンク
- １１０ 登録オーソリティ
- １１１ データベース
- ２００，２０２ 不揮発性ストレージデバイス
- ２０４ 処理ユニット
- ２１０，２１２ バックアップ電源
- ３００ 通信インターフェース
- ３０２ センサコントローラ
- ３０４ 不揮発性ストレージコントローラ
- ３０６ プロセッサ
- ３０８ 揮発性メモリ
- ３１０ 不揮発性メモリ
- ４００，５１６ ストレージＩＤ情報
- ４０２ ディレクトリ情報
- ４０４ データ
- ４２０ 登録識別子値
- ４２２ ヘッダ・セグメント
- ４２４ デバイス・メーカー・セグメント
- ４２６ シリアル・ナンバー・セグメント
- ４６０ テーブル
- ４６２ 行
- ４６４～４６８ 列
- ５００，５１２ ディレクトリエントリ
- ５０２ ファイル名
- ５０４ 作成日付

30

40

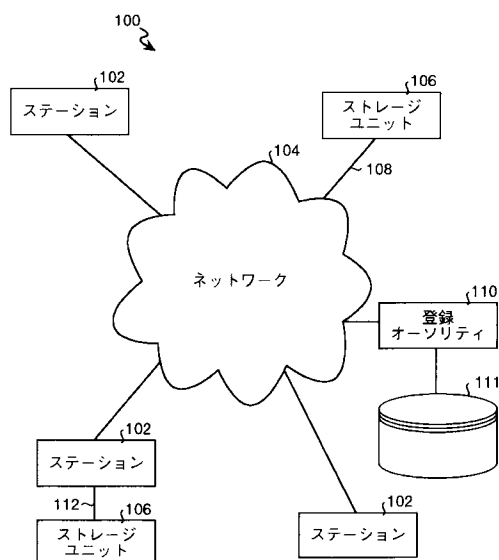
50

506 有効期限
 508 他のファイル管理情報
 510 複製情報
 512 ディレクトリエントリ
 514 複製日付
 602 バス
 604 プロセッサ
 606 メインメモリ
 608 ROM
 610 ストレージデバイス
 612 ディスプレイ
 614 入力デバイス
 616 カーソルコントロール
 618 通信インターフェース
 620 ネットワークリンク
 622 ローカルネットワーク
 624 ホストコンピュータ
 626 ISP
 628 インターネット
 630 サーバ
 S1～S4 センサ

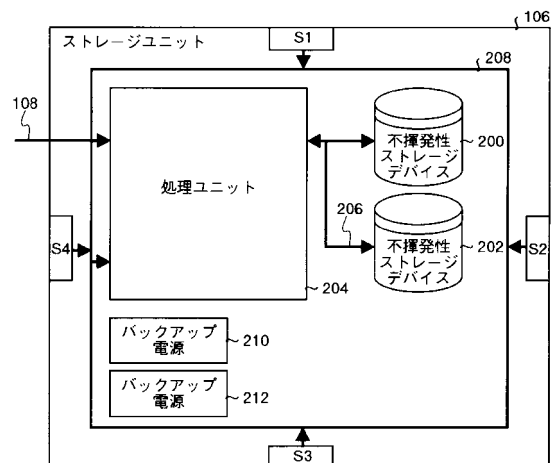
10

20

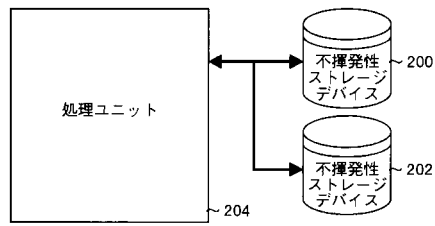
【図1】



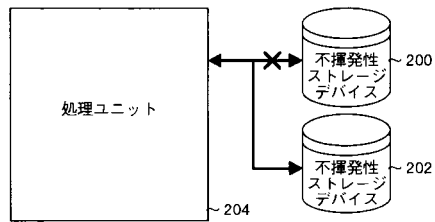
【図2】



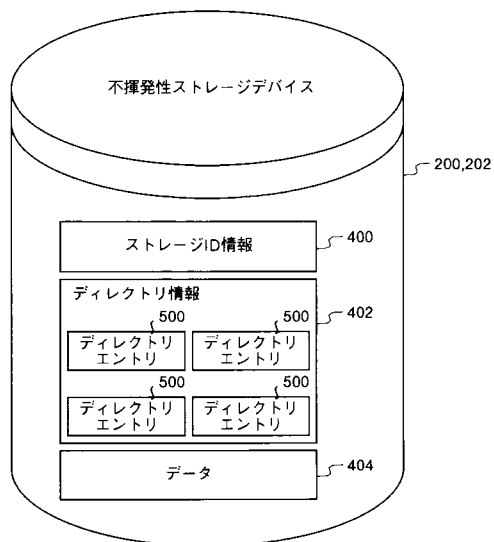
【図 3】



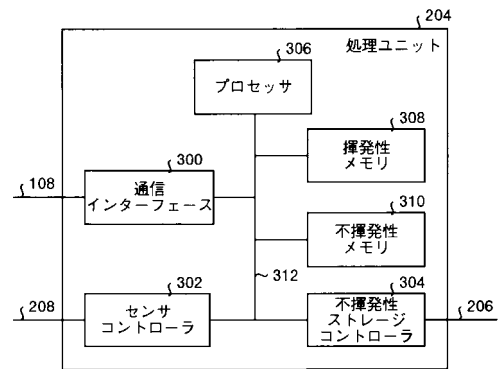
【図 4】



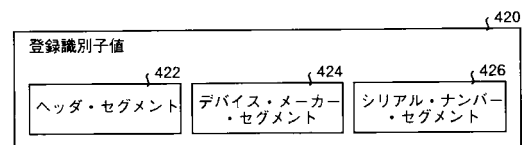
【図 6】



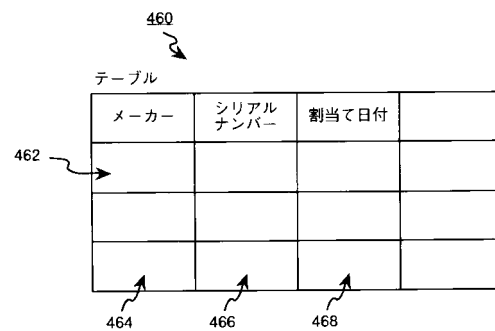
【図 5】



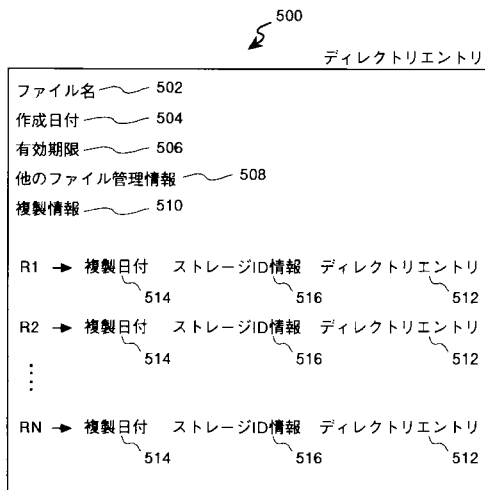
【図 7】



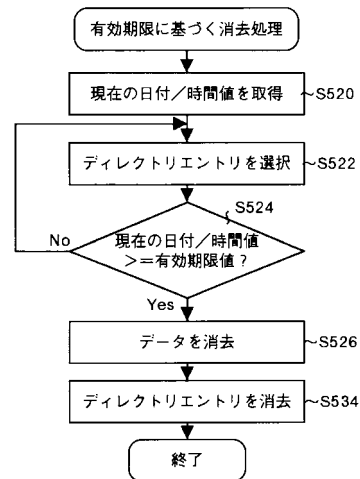
【図 8】



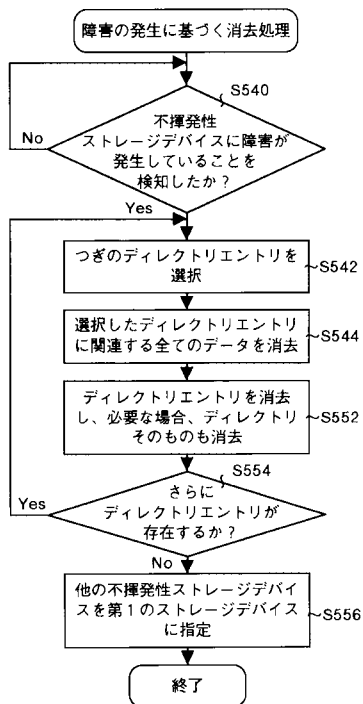
【図 9】



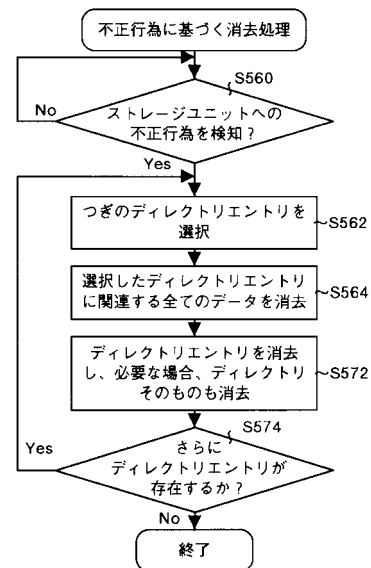
【図 10】



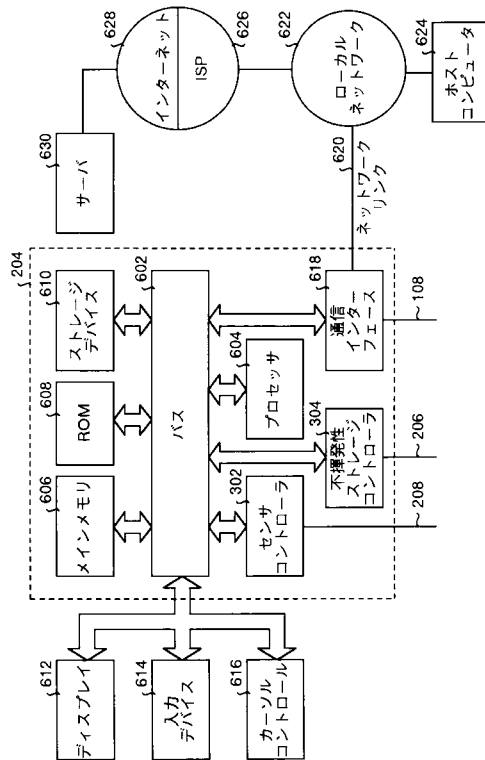
【図 11】



【図 12】



【図 13】



フロントページの続き

審査官 小林 秀和

(56)参考文献 国際公開第92/09946 (WO, A1)

米国特許第04634807 (US, A)

特開平10-134279 (JP, A)

特開平05-197459 (JP, A)

特開平09-311822 (JP, A)

特開昭64-053241 (JP, A)

特開平04-340336 (JP, A)

実開昭63-107049 (JP, U)

特開平11-095933 (JP, A)

特開平08-138307 (JP, A)

特開平10-181786 (JP, A)

Alastair McLeod, "Digital Video Storage for Security Applications", Security Technology, 1995. Proceedings. Institute of Electrical and Electronics Engineers 29th Annual 1995 International Carnahan Conference on, 英国, 1995年10月20日, p.382-p.387, ISBN: 0-7803-2627-X

(58)調査した分野(Int.Cl., DB名)

G06F 21/24

G06F 3/06