

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第4864330号
(P4864330)

(45) 発行日 平成24年2月1日 (2012. 2. 1)

(24) 登録日 平成23年11月18日 (2011. 11. 18)

(51) Int. Cl.	F I
GO 6 F 21/24 (2006. 01)	GO 6 F 12/14 5 6 O C
GO 6 F 12/10 (2006. 01)	GO 6 F 12/14 5 4 O A
GO 6 F 13/10 (2006. 01)	GO 6 F 12/10 5 5 9
GO 9 C 1/00 (2006. 01)	GO 6 F 13/10 3 4 O A
	GO 9 C 1/00 6 4 O D

請求項の数 51 (全 30 頁)

(21) 出願番号	特願2005-33676 (P2005-33676)	(73) 特許権者	500232617
(22) 出願日	平成17年2月9日 (2005. 2. 9)		イルデト・ペー・フェー
(65) 公開番号	特開2005-243013 (P2005-243013A)		オランダ・N L-2 1 3 2・L S・フーフ
(43) 公開日	平成17年9月8日 (2005. 9. 8)		ドローブ・タウルサヴェンウー・1 0 5
審査請求日	平成20年1月30日 (2008. 1. 30)	(74) 代理人	100064908
(31) 優先権主張番号	04100546.3		弁理士 志賀 正武
(32) 優先日	平成16年2月12日 (2004. 2. 12)	(74) 代理人	100089037
(33) 優先権主張国	欧州特許庁 (EP)		弁理士 渡邊 隆
		(74) 代理人	100108453
			弁理士 村山 靖彦
		(74) 代理人	100110364
			弁理士 実広 信哉

最終頁に続く

(54) 【発明の名称】 外部データの記憶方法及びシステム

(57) 【特許請求の範囲】

【請求項 1】

プロセッサ（ 2 ； 7 4 ） 、 及び該プロセッサ（ 2 ； 7 4 ） におけるアクティブ記録を処理するよう適合された一次データ記憶ユニット（ 4 ； 7 7 ） を有し、 該一次データ記憶ユニット（ 4 ； 7 7 ） にアクティブ記録に属するデータを記憶するよう構成された一次処理装置（ 1 ； 7 2 ） と、 一次処理装置（ 1 ； 7 2 ） にアクセス可能な二次データ記憶システム（ 5 ； 5 7 , 6 9 ） とを含むシステムにおいて外部データ記憶を可能とする方法であって、

前記アクティブ記録は、 一次処理装置（ 1 ； 7 2 ） によって実行される少なくとも 1 つの応用プログラムによってアクティブにされた記録であり、

前記方法は、
一次データ記憶ユニット（ 4 ； 7 7 ） が応用プログラムによってアクティブにされた記録に属するデータを記録するステップと、

応用プログラム・インターフェースが、 前記記録に属するデータ（ 3 4 ） の少なくとも 1 つの項目を記憶のために二次データ記憶システム（ 5 ； 5 7 , 6 9 ） に転送することにより前記記録を外部化するステップと、
を含み、

前記記録を外部化する該ステップは、 前記応用プログラム・インターフェースが、 前記記録に属するデータを用いて前記応用プログラムにより開始される少なくとも 1 つの呼び出しの受信をすることを含む方法。

【請求項 2】

前記データ(34)の項目は、複数の部分(35-37)に分割され、

前記方法は、さらに、

前記一次処理装置(1;72)が、データ(34)の1つの項目だけのなかの複数の部分(35-37)における少なくとも1つの部分に対応するデータ(41-43)を含むデータ・セクション(48,52,56)を識別する情報を含む少なくとも1つの外部化メッセージを受信し、そして該外部化メッセージに回答して、少なくとも識別されたデータ・セクション(48,52,56)を転送することを含む請求項1に記載の方法。

【請求項 3】

前記一次処理装置(1;72)が、データ(34)の項目を複数の部分(35-37)に分割し、複数の外部化メッセージを受信することを含む、

複数の外部化メッセージにおける各外部化メッセージは、複数の部分(35-37)の一部分に対応するデータ(41-43)を含むデータ・セクション(48,52,56)を識別し、そして各外部化メッセージに回答して少なくとも識別されたデータ・セクションを転送することを含む請求項1または2に記載の方法。

【請求項 4】

部分(35-37)に対応するデータ(41-43)は、データ(34)の項目の部分(35-37)を少なくとも部分的に暗号化することにより発生される請求項2または3に記載の方法。

【請求項 5】

前記一次処理装置(1;72)が、データ(34)の項目を連続する部分(35-37)のシーケンスに分割し、一連の外部化メッセージを受信し、シーケンスにおける対応部分(35-37)の位置によってデータ・セクション(48,52,56)を識別する情報及び記録を識別する情報を各々含め、そして二次記憶システム(5;57,69)に転送する前にデータ・セクション(48,52,56)にデータ・セクション(48,52,56)を識別する情報に対応するデータを含めることを含む請求項3または4に記載の方法。

【請求項 6】

前記一次処理装置(1;72)が、アプリケーションからの呼び出しに回答してシーケンス内にいかに多くの部分(35-37)が存在するかを表す情報を戻すことを含む請求項5に記載の方法。

【請求項 7】

前記一次処理装置(1;72)が、データ(34)の項目の複数の部分(35-37)における各部分のための認証値(45,49,54)を計算し、該複数の部分(35-37)の部分に対応するデータ(41-43)を含むデータ・セクション(48,52,56)に認証値(45,49,54)を反映させるデータを含めることを含む請求項2乃至6のいずれかに記載の方法。

【請求項 8】

前記一次処理装置(1;72)が、入力としてのさらなる部分(35,36)から導出された情報を用いて少なくとも1つの部分(36-37)のための認証値(49,54)を計算することを含む請求項3または7に記載の方法。

【請求項 9】

一次装置(1)のデータ記憶ユニット(4)が、各外部化された記録ごとに基準データ・オブジェクト(11)を記憶し、独特の識別子を含めることを含み、該独特の識別子を反映するデータは、記録に属するデータ(34)の項目の部分(35-37)に対応するデータ(41-43)を含む各データ・セクション(48,52,56)に含まれる請求項2乃至8のいずれかに記載の方法。

【請求項 10】

プロセッサ(2;74)、及び該プロセッサ(2;74)においてアクティブ記録を処理するためのアプリケーションプログラムを走行させるよう適合された一次データ記憶ユニット(4;

10

20

30

40

50

77)を有し、該一次データ記憶ユニット(4;77)にアクティブ記録に属するデータを記憶するよう構成された一次処理装置(1;72)と、一次処理装置(1;72)にアクセス可能な二次データ記憶システム(5;57,69)とを含むシステムにおける外部データ記憶の方法であって、

前記アクティブ記録は、一次処理装置(1;72)によって実行される少なくとも1つの応用プログラムによってアクティブにされた記録であり、

前記アクティブ記録に属するデータを、一次データ記憶ユニット(4;77)にローディングするステップ、及び

記録に属するデータの少なくとも項目(34)を記憶のために二次データ記憶システム(5;57,69)に転送することにより記録を外部化するステップ、

を含み、該記録を外部化するステップは、データ・項目(34)を二次データ記憶システム(5;57,69)に転送するよう適合されたインターフェース(6-8;60、61、62、66、70、78)に、記録に属するデータを用いて応用プログラムにより呼び出しを行うことを含む方法。

【請求項11】

記録に属するデータの1つの項目(34)だけの少なくとも部分(35-37)に対応するデータ(41-43)を含むデータ・セクション(48、52、56)を転送することを含む請求項10に記載の方法。

【請求項12】

データの項目(34)は、複数の部分(35-37)に分割され、複数の部分(35-37)の1つに対応するデータ(41-43)を各々が含む複数のデータ・セクション(48、52、56)は、記憶のために二次データ記憶システム(5;57,69)に転送される請求項10または11に記載の方法。

【請求項13】

部分(35-37)に対応するデータ(41-43)は、データ(34)の項目の部分(35-37)を少なくとも部分的に暗号化することにより発生される請求項11または12に記載の方法。

【請求項14】

データの項目(34)の各部分(35-37)ごとに認証値(45、49、54)を計算し、そして該部分(35-37)に対応するデータ(41-43)を含むデータ・セクション(48、52、56)に認証値(45、49、54)を反映するデータを含めることを含む請求項11乃至13のいずれかに記載の方法。

【請求項15】

入力としてさらなる部分(35、36)から導出された情報を用いてデータの項目(34)の少なくとも1つの部分(36-37)のための認証値を計算することを含む請求項14に記載の方法。

【請求項16】

各外部化された記録ごとに一次装置(1)のデータ記憶ユニット(4)に基準データ・オブジェクト(11)を記憶し、独特の識別子を含めることを含み、該独特の識別子を反映するデータは、記録に属するデータの項目(34)の部分(35-37)に対応するデータ(41-43)を含む各データ・セクションに含まれる請求項11乃至15のいずれかに記載の方法。

【請求項17】

外部化された記録のためのバージョン・カウントを反映する情報を記憶し、そして記録を外部化する前にバージョン・カウントを増分することを含む請求項10乃至16のいずれかに記載の方法。

【請求項18】

プロセッサ(2;74)、及び該プロセッサ(2;74)におけるアクティブ記録を処理するよう適合された一次データ記憶ユニット(4;77)を有し、該一次データ記憶ユニット(4;77)にアクティブ記録に属するデータを記憶するよう構成された一次処理

10

20

30

40

50

装置（１；７２）と、一次処理装置（１；７２）にアクセス可能な二次データ記憶システム（５；５７、６９）とを含み、請求項１０乃至１７のいずれかに記載の方法により転送されたデータの項目（３４）を記憶するよう適合されたシステムにおいて記録を内部化する方法であって、

前記アクティブ記録は、一次処理装置（１；７２）によって実行される少なくとも１つの応用プログラムによってアクティブにされた記録であり、

該方法は、記録に属するデータを、一次データ記憶ユニット（４；７７）にローディングするステップを含み、

前記システムは、二次データ記憶システム（５；５７、６９）から記録に属するデータの項目（３４）を検索するためのインターフェース（６－８；６０、６１、６２、６６、

10

７０、７８）を含み、
前記方法は、さらに、記録に属するデータを用いるよう構成された応用プログラムが、記録が内部化されるべきであることを決定し、そしてインターフェース（６－８；６０、６１、６２、６６、７０、７８）への少なくとも１つの呼び出しを行うというステップを含む方法。

【請求項１９】

二次記憶システム（５；５７、６９）からデータの１つの項目（３４）の少なくとも部分（３５－３７）に対応するデータ（４１－４３）を含む少なくとも１つのデータ・セクション（４８、５２、５６）を受信することを含む請求項１８に記載の方法。

【請求項２０】

20

一次処理装置（１）のデータ記憶ユニット（４）に記憶された基準オブジェクト（１１）から記録に独特の識別子を検索するステップを含み、ここに、データ・セクション（４８、５２、５６）は、独特の識別子を反映する情報と共に二次データ記憶システム（５；５７、６９）に記憶され、そして独特の識別子を反映する情報を含む内部化メッセージに応答して受信される請求項１９に記載の方法。

【請求項２１】

データの項目（３４）は複数の部分（３５－３７）を含み、

複数の部分（３５－３７）の１つに対応するデータ（４１－４３）を各々が含む多くのデータ・セクション（４８、５２、５６）を受信するステップを含む請求項１８乃至２０のいずれかに記載の方法。

30

【請求項２２】

基準オブジェクト（１１）から部分（３５－３７）の数を反映する情報を検索すること、及び対応する内部化メッセージに**応答して**各データ・セクション（４８、５２、５６）を受信することを含む請求項２０または２１に記載の方法。

【請求項２３】

認証値（４５、４９、５４）を含む少なくとも１つのデータ・セクション（４８、５２、５６）を受信すること、一次処理装置（１）に記憶された情報（４６）の秘密項目を検索すること、入力としての情報（４６）の秘密項目を用いて、データの項目（３４）の少なくとも部分（３５－３７）に対応するデータ（４１－４３）の少なくとも部分から各データ・セクション（４８、５２、５６）のための確認認証値を計算すること、並びに各データ・セクション（４８、５２、５６）ごとに確認認証値と認証値（４５、４９、５４）とを比較することを含む請求項１９乃至２２のいずれかに記載の方法。

40

【請求項２４】

各々が認証値（４５、４９、５４）を含むデータ・セクション（４８、５２、５６）のシーケンスを受信することを含み、少なくとも１つのデータ・セクション（４８、５２、５６）のための確認認証値は、入力としてさらなるデータ・セクション（４８、５２、５６）から導出された情報（４５、４９）を用いて計算される請求項２３に記載の方法。

【請求項２５】

一次処理装置（１）に記憶された秘密キー（４０）を検索すること、及び受信されたデータ・セクション（４８、５２、５６）の少なくとも部分（４１－４３）を解読すること

50

を含む請求項 19 乃至 24 のいずれかに記載の方法。

【請求項 26】

外部化された記録のためのバージョン・カウントを反映する情報を含むデータ・セクション(48、52、56)を受信すること、及び該バージョン・カウントを基準バージョン・カウントと比較することを含む請求項 19 乃至 25 のいずれかに記載の方法。

【請求項 27】

プロセッサ(2;74)、及び該プロセッサ(2;74)におけるアクティブ記録を処理するよう適合された一次データ記憶ユニット(4;77)を有し、該一次データ記憶ユニット(4;77)に1つのアクティブ記録に属するデータを記憶するよう構成された一次処理装置(1;72)と、一次処理装置(1;72)にアクセス可能な二次データ記憶システム(5;57,69)とを含み、請求項 10 乃至 17 のいずれかに記載の方法により転送されたデータの項目(34)を記憶するよう適合されたシステムにおいて記録の内部化を可能とする方法であって、

前記アクティブ記録は、一次処理装置(1;72)によって実行される少なくとも1つの応用プログラムによってアクティブにされた記録であり、

1つのアクティブ記録に属するデータは、一次データ記憶ユニット(4;77)にロードされ、かつ記録は、記録に属するデータの少なくとも項目(34)を二次データ記憶システム(5;57,69)から検索することにより内部化され、

記録を内部化する該ステップは、記録に属するデータを用いて応用プログラムにより開始される少なくとも1つの呼び出しを、二次データ記憶システム(5;57,69)からデータの項目を検索するよう適合された応用プログラム・インターフェースにより受信することを含む方法。

【請求項 28】

データの項目(34)の少なくとも部分(35-37)に対応するデータ(41-43)を含むデータ・セクション(48、52、56)を識別する情報を含む少なくとも1つの内部化メッセージを、前記応用プログラムから前記二次データ記憶システム(5;57,69)が受信すること、並びに内部化メッセージに回答して少なくとも該識別されたデータ・セクション(48、52、56)を検索することを含む請求項 27 に記載の方法。

【請求項 29】

データの項目(34)は、複数の部分(35-37)を備え、当該方法は、複数の部分(35-37)の1つに対応するデータ(41-43)を含むデータ・セクション(48、52、56)を各々が識別する、複数の内部化メッセージを受信すること、並びに各内部化メッセージに回答して少なくとも識別されたデータ・セクション(48、52、56)を検索することを含む請求項 27 または 28 に記載の方法。

【請求項 30】

各転送されたデータ・セクション(48、2、56)の少なくとも部分を解読することを含み、解読された該部分は、データの項目(34)の部分(35-37)に対応するデータ(41-43)の少なくとも部分を含む請求項 28 または 29 に記載の方法。

【請求項 31】

データの項目(34)が連続する部分(35-37)の順番付けられたシーケンスを含み、当該方法は、該シーケンスにおける部分(35-37)の位置により記録を識別する情報及びデータ・セクション(48、52、56)を識別する情報を各々が含む、一連の内部化メッセージを受信することを含む請求項 29 または 30 に記載の方法。

【請求項 32】

データの項目(34)の各部分(35-37)ごとに基準認証値を計算すること、並びに該基準認証値を、当該部分(35-37)に対応するデータ・セクション(48、52、56)に含まれる認証値を反映するデータと比較することを含む請求項 28 乃至 31 のいずれかに記載の方法。

【請求項 33】

入力としてさらなる部分(35-36)から導出された情報を用いて少なくとも1つの

10

20

30

40

50

部分(36-37)のための基準認証値を計算することを含む請求項29または32に記載の方法。

【請求項34】

プロセッサ(2;74)、及び該プロセッサ(2;74)においてアクティブ記録を処理するよう適合された一次データ記憶ユニット(4;77)を有し、該一次データ記憶ユニット(4;77)にアクティブ記録に属するデータを記憶するよう構成された一次処理装置(1;72)と、一次処理装置(1;72)にアクセス可能な二次データ記憶システム(5;57,69)とを含むシステムにおける外部データ記憶の方法であって、該方法は、

前記アクティブ記録は、一次処理装置(1;72)によって実行される少なくとも1つの応用プログラムによってアクティブにされた記録であり、

アクティブ記録に属するデータを、一次データ記憶ユニット(4;77)にローディングするステップ、及び

記録に属するデータの少なくとも項目(34)を記憶のために二次データ記憶システム(5;57,69)に転送することにより記録を外部化するステップ、

を含み、該方法は、

前記二次データ記憶システム(5;57,69)が、外部化された記録のためのバージョン・カウントを反映する情報を記憶するステップ、及び

記録を外部化するに先立ってバージョン・カウントを増分するステップを含む方法。

【請求項35】

独特の識別子、及びバージョン・カウントを反映する情報のコピーを含む、各外部化された記録ごとに、一次処理装置(1;72)のデータ記憶ユニット(4;77)に基準データ・オブジェクトを記憶することを含む請求項34に記載の方法。

【請求項36】

データの項目(34)の少なくとも部分(35-37)に対応するデータ及びバージョン・カウントを反映する情報に対応するデータを含む少なくとも1つのデータ・セクション(48,52,56)を二次データ記憶システム(5;57,69)に転送することを含む請求項34または35に記載の方法。

【請求項37】

一次データ記憶ユニット(4;77)にローディングした後アクティブ記録に属するデータのいずれかが変化されたか否かを決定すること、並びにアクティブ記録に属する或るデータが変化されたことを決定した後だけにバージョン・カウントを増分することを含む請求項34乃至36のいずれかに記載の方法。

【請求項38】

一次データ記憶ユニット(4;77)にローディングした後記録に属する何等かのデータが修正された場合にアクティブ記録におけるフラッグをセットすることを含み、フラッグがセットされてしまったということを決定した後だけに記録が外部化される請求項34乃至37のいずれかに記載の方法。

【請求項39】

プロセッサ(2;74)、及び該プロセッサ(2;74)におけるアクティブ記録を処理するよう適合された一次データ記憶ユニット(4;77)を有し、該一次データ記憶ユニット(4;77)に1つのアクティブ記録に属するデータを記憶するよう構成された一次処理装置(1;72)と、一次処理装置(1;72)にアクセス可能な二次データ記憶システム(5;57,69)とを含み、請求項34乃至38のいずれかに記載の方法により転送されたデータの項目(34)を記憶するよう適合されたシステムにおいて記録を内部化する方法であって、

前記アクティブ記録は、一次処理装置(1;72)によって実行される少なくとも1つの応用プログラムによってアクティブにされた記録であり、

データの項目(34)の少なくとも部分(35-37)に対応するデータ(41-43)を含む少なくとも1つのデータ・セクション(48,52,56)は、二次データ記憶

10

20

30

40

50

システム（５；５７，６９）から検索され、

外部化された記録のためのバージョン・カウントを反映する情報を含むデータ・セクション（４８、５２、５６）が受信され、そしてバージョン・カウントは基準バージョン・カウントと比較される方法。

【請求項４０】

データの項目（３４）の部分（３５－３７）は、データ・セクション（４８、５２、５６）に含まれた対応のデータ（４１－４３）からだけ検索され、もしバージョン・カウントが基準バージョン・カウントに対応したならば、一次データ記憶ユニット（４；７７）にローディングされる請求項３９に記載の方法。

【請求項４１】

一次処理装置（１）のデータ記憶ユニット（４；７７）に記憶された、外部化された記録のための基準データ・オブジェクト（１１）から基準バージョン・カウントを検索することを含む請求項３９または４０に記載の方法。

【請求項４２】

信頼のできる第三者のシステムから基準バージョン・カウントを受信することを含む請求項３９乃至４１のいずれかに記載の方法。

【請求項４３】

二次記憶システム（５；５７，６９）から基準バージョン・カウントを受信することを含む請求項３９乃至４１のいずれかに記載の方法。

【請求項４４】

イベントを形成するデジタル内容の少なくとも１つの連続する項目へのアクセスを提供するよう適合され、かつ少なくとも１つの記録に含まれる情報に従ってイベントへのアクセスを制御するよう適合された条件付けアクセス・サブシステム（６９、７２）を含むマルチメディア・システム（５７、６９、７２）において記録を処理する方法であって、

マルチメディア・システム（５７、６９、７２）は、

イベントがアクセスされているときにプロセッサ（７４）においてアクティブ記録を処理するための少なくとも１つの応用プログラムを走行させるよう適合された、プロセッサ（７４）及び一次データ記憶ユニット（７７）を有して、一次データ記憶ユニット（７７）にアクティブ記録に属するデータを記憶するよう構成された安全一次処理装置（７２）と、

一次処理装置（７２）にアクセス可能な二次データ記憶システム（５７、６９）と、を含む場合において、

請求項１乃至４３のいずれかに記載の方法を適用したことを特徴とする方法。

【請求項４５】

或るイベントに対応した少なくとも１つのイベント記録を、前記イベントがアクセスされているときにアクティブにすることを含む請求項４４に記載の方法。

【請求項４６】

イベント記録は、再生カウントを反映する情報を含み、当該方法は、イベント記録がアクティブにされているときに再生カウントを増分することを含む請求項４５に記載の方法。

【請求項４７】

イベントへのアクセスは、該イベントに対応するセッション中に提供され、当該方法は、前記セッションの間に該セッションに対応するセッション記録をアクティブにする請求項４４乃至４６のいずれかに記載の方法。

【請求項４８】

セッションの間に、前記イベントへのアクセスを提供するための暗号化されたデータを受信すること、前記セッション記録から少なくとも１つのキー（４０）を検索すること、暗号化されたデータを解読すること、並びに解読されたデータを戻すことを含む請求項４７に記載の方法。

【請求項４９】

10

20

30

40

50

セッションの間に、イベントへのアクセスを提供するためのアクセス・データを受信すること、並びにイベントに対応するセッションに対応するセッション記録にアクセス・データを記憶することを含む請求項 47 に記載の方法。

【請求項 50】

プロセッサ(2; 74)及び該プロセッサ(2; 74)においてアクティブ記録を処理するよう適合された一次データ記憶ユニット(4; 77)を有する一次処理装置であって、一次データ記憶ユニット(4; 77)にアクティブ記録に属するデータを記憶するよう構成され、かつ請求項 1 乃至 49 のいずれかに記載の方法を実行するよう適合された一次処理装置。

【請求項 51】

プロセッサ(2; 74)及び一次データ記憶ユニット(4; 77)を有する一次処理装置(1; 72)によって走行されるとき、該一次処理装置(1; 72)が請求項 1 乃至 49 のいずれかに記載の方法を実行するのを可能とするコンピュータ・プログラム手段。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、概して、処理装置によって処理されたデータを外部的に記憶する方法に関する。特に、本発明は、外部データの記憶方法、データを内部化する方法、並びに外部データの記憶及びデータの内部化を可能にする方法に関する。本発明は、また、該方法をマルチメディア・システムに適用すること、並びに該方法を実行するためのシステム及びコンピュータ・プログラムに関する。

【背景技術】

【0002】

外部データ記憶を可能とする方法、外部データの記憶方法並びに該方法を行うように適合されたシステムの例は、例えば、US 5,757,919 から知られている。この公報は、物理的に安全な環境から外部記憶ユニットにページングされるページの完全性及び機密性を維持するための方法及びシステムを開示している。この物理的に安全な環境は、バスによってランダム・アクセス・メモリに結合された保証プロセッサを含む。完全性チェック・エンジンは、安全な環境と、安全でない環境、特に外部記憶ユニットとの間で、データ・ページングの一方向ハッシュ(hash)を行う。一実施形態では、保証プロセッサは、1Kページを用いるよう構築されている。安全でない環境におけるホスト・プロセッサは、外部メモリに記憶されている保証プロセッサのページを1Kデータ・ブロックとして扱う。ページが必要に応じて識別されるならば、該ページが保証メモリ内に存在するかどうかの決定が為される。該ページが存在するならば、ページ・ヒットが生じ、さらなる動作は必要とされない。ページが存在しないならば、ページ・フォルトが生じる。ページ・フォルトが生じると、必要とされるページがマッピングされ得るスペースが保証メモリ内に得られるかどうかの決定が為される。スペースが得られないならば、次に、ページ・アウトするためのページが選択される。最近殆ど使用されていないというような、種々の選択規準が用いられ得る。

【0003】

既知の方法及びシステムは、二次データ記憶システムに運ばれるべきデータのピースを選択することが困難であるという欠点を有する。ページ・イン及びページ・アウトを行うには概して待ち時間を含み、ページ・フォルトの場合には保証サービスが待ち時間を増加させるので、このことは、能動(アクティブ)記録の処理を減速させる。

【0004】

外部データの記憶、データを内部化する方法、マルチメディア・システムにおける記録を処理する方法、並びにかかる方法を行うのに適合したシステムのもう1つの例は、FR-A-2,803,471 に開示されている。この公報は、テレビジョン受信機におけるメモリ管理プロセスを開示している。テレビジョン・システムは、テレビジョンと、該テレビジョンに埋設された局部メモリ手段と、メモリ・カードまたはディスク・ドライブの

10

20

30

40

50

ような、テレビジョンと関連した外部メモリ手段とを備える。該システムは、複数の実行可能なモジュールを含むコンピュータ・プログラムを含む。第1のモジュールは、情報を記憶させる各要求を受信して分析する。メモリ手段の特性が、新しい情報の記憶を許容しないならば、第1のモジュールは、第2のモジュールをトリガする。第2のモジュールは、記憶された情報の使用規準を尊重しつつメモリ・スペースを開放する。第1及び第2のモジュールは、情報の記憶を最適化するために一連の単純な手順を用いる。これらの手順は、例えば、第1のメモリ手段から第2のメモリ手段へのデータの移動を実現する。

【0005】

この既知のシステム及び方法の問題点は、外部化されてしまうと、記録の部分のまたはすべての処理を許容しないということである。このことが起こり、後の段においてテレビジョンに転送し戻されるならば、記録に属するデータの完全なセットは、外部化の前にテレビジョン・セットに適用することによって最後に処理されたデータの完全なセットと同一ではないであろう。

【特許文献1】US 5 757 919

【特許文献2】FR - A - 2 803 471

【発明の開示】

【課題を解決するための手段】

【0006】

本発明は、外部データ記憶を可能にする方法、外部データ記憶の方法、記録を内部化する方法、記録の内部化を可能にする方法、一次処理装置、並びに二次記憶システムへの及びそれからのデータの転送の数に関して一層効率的なコンピュータ・プログラム手段を提供する。

【0007】

これは、以下に述べる外部データ記憶を可能とする方法を提供することによって達成される。すなわち、プロセッサ、及び該プロセッサにおけるアクティブ記録を処理するよう適合された一次データ記憶ユニットを有し、該一次データ記憶ユニットにアクティブ記録に属するデータを記憶するよう構成された一次処理装置と、一次処理装置にアクセス可能な二次データ記憶システムとを含むシステムにおいて外部データ記憶を可能とする方法であって、

アクティブ記録に属するデータは、一次データ記憶ユニットに記憶され、かつ記録は、アクティブ記録に属するデータの少なくともピースを記憶のために二次データ記憶システムに転送することにより外部化され、

記録を外部化する該ステップは、記録に属するデータを用いて応用プログラムにより開始される少なくとも1つの呼び出しを、二次データ記憶システムにデータのピースを送るよう配列された応用プログラム・インターフェースにより受信することを含む方法を提供することによって達成される。

【0008】

従って、転送されるデータのピースは記録に属するので、当該方法は、一次処理装置のプロセッサが、プロセッサにより走行されるプロセスに利用可能なメモリ・アドレスに基づく手法よりも、記録に属するデータにアクセスすることが必要であろうという事実を一層良く考慮している。外部化(externalisation)は、記録に属するデータを実際用いて応用プログラムにより開始されるので、どの記録が、従って、どのデータのピースが、近い将来において一次処理装置で必要とされそうかということを予測することが一層容易である。

【0009】

本発明は、仮想メモリ・アドレスを物理アドレスに関係付けるためのどんなページ・テーブルも必要ではないという追加の利点を有する。

【0010】

好適な実施形態は、データの1つのピースだけの少なくとも関連部分に対応するデータを含むデータ・セクションを識別する情報を含む少なくとも1つの外部化メッセージを受

10

20

30

40

50

信すること、並びに該外部化メッセージに応答して、少なくとも識別されたデータ・セクションを転送することを含む。

【 0 0 1 1 】

このように、記憶のために二次記憶システムに転送される各データ・セクションは、データの1つのピースだけの関連部分に対応するデータを含む。1つ以上の記録が外部化されるべきである場合には、このことは、1つの記録に属するデータに対応するサブセクション及びさらなる記録に属するデータに対応するサブセクションと共にデータ・セクションを記憶することを排除する。換言すれば、1つの記録に属するデータに対応するデータは、常に、もう1つの記録に属するデータに対応するデータとは別のデータ・セクションに記憶される。実施形態は、二次記憶システムへの、そして特にからの不必要なデータ転送を除去する利点を有する。

10

【 0 0 1 2 】

好適な実施形態は、データのピースを複数の部分に分割し、複数の外部化メッセージを受信し、複数の部分の関連部分に対応するデータを含むデータ・セクションを各々識別し、そして各外部化メッセージに応答して少なくとも識別されたデータ・セクションを転送することを含む。

【 0 0 1 3 】

この実施形態は、一次処理装置に利用可能な主メモリのサイズ、及び/またはデータ・パイプラインの幅のような二次記憶システムへのインターフェースの特性に適合可能である利点を有する。

20

【 0 0 1 4 】

好適な実施形態において、関連部分に対応するデータは、データのピースの関連部分を少なくとも部分的に暗号化することにより発生される。

【 0 0 1 5 】

記憶のために二次記憶システムに転送されるデータ・セクションは、少なくとも部分的に暗号化されるので、一次データ記憶ユニット、及び一次データ処理装置のプロセッサだけが、データの全体の完全な安全性を維持するために、安全環境に安置されることが必要である。一次処理装置は、制限された記憶容量を有する一次記憶ユニットだけを有することが必要であるので、データを外部的に記憶する可能性のために、かかる安全環境を提供することが一層安価でありかつ容易である。

30

【 0 0 1 6 】

好適な実施形態は、データのピースを連続する部分のシーケンスに分割し、一連の外部化メッセージを受信し、シーケンスにおける対応部分の位置によってデータ・セクションを識別する情報及び記録を識別する情報を各々含め、そして二次記憶システムに転送する前にデータ・セクションにデータ・セクションを識別する情報に対応するデータを含めることを含む。

【 0 0 1 7 】

この実施形態は、データ・セクションが再度読み出されるべきである順番を記載している情報が二次記憶システムに記憶されるという利点を有する。このように、非常に制限された容量を有する一次処理装置、特に制限された揮発性主メモリにおいて、一次記憶ユニットにローディング・バックされるべきデータのピースの部分は、構成部分、すなわち部分が関連しているデータ・セクションをバッファリングする必要なく、順次的に処理される。

40

【 0 0 1 8 】

好ましくは、当該方法は、データのピースの各部分のための認証値を計算し、該部分と対応したデータを含むデータ・セクションに認証値を反映させるデータを含めることを含む。

【 0 0 1 9 】

このように、データ・セクションにおけるデータ、特に、データ・セクションと関連するデータのピースの部分に対応するデータが改ざんされてしまったか否かを後の段階で決

50

定することを可能とする。

【0020】

本発明のもう1つの態様によれば、プロセッサ、及び該プロセッサにおいてアクティブ記録を処理するための応用プログラムを走行させるよう適合された一次データ記憶ユニットを有し、該一次データ記憶ユニットにアクティブ記録に属するデータを記憶するよう構成された一次処理装置と、一次処理装置にアクセス可能な二次データ記憶システムとを含むシステムにおける外部データ記憶の方法であって、

アクティブ記録に属するデータを、一次データ記憶ユニットにローディングするステップ、及び

記録に属するデータの少なくともピースを記憶のために二次データ記憶システムに転送することにより記録を外部化するステップ、

を含み、該記録を外部化するステップは、データ・ピースを二次データ記憶システムに転送するよう配列されたインターフェースに、記録に属するデータを用いて応用プログラムにより呼び出しを行うことを含む方法が提供される。

【0021】

当該方法が適用されるとき、記録に属するデータの外部記憶に渡る制御は、データを実際に用いている応用プログラムに転送される。呼び出しは、本発明による外部データ記憶を可能とする方法を行うよう適合された応用プログラム・インターフェースに対して為される。代替的には、当該方法は、一次処理装置で走行している応用プログラムによって直接行われ得る。従って、それは、記録が外部化されているか否かを決定するよう応用プログラムを可能化する利点を与える。このように、応用プログラムは、近い将来に処理しているであろう記録に属するデータのピースが、二次記憶装置に転送されることを阻止することができる。応用プログラムの実行は、このように、スピードアップされ、その理由は、記録を外部化し、それが再度修正されるべきであるときに二次記憶システムからデータのピースを引き続き検索することと関連した待ち時間が回避されるからである。

【0022】

好ましくは、当該方法は、記録に属するデータの1つのピースだけの少なくとも関連部分に対応するデータを含むデータ・セクションを転送することを含む。

【0023】

このように、記憶のために二次記憶システムに転送される各データ・セクションは、データの1つのピースだけの関連部分に対応するデータを含む。1つ以上の記録が外部化されるべきである場合には、このことは、1つの記録に属するデータに対応するサブセクション及びさらなる記録に属するデータに対応するサブセクションと共にデータ・セクションを記憶することを排除する。換言すれば、1つの記録に属するデータに対応するデータは、常に、もう1つの記録に属するデータに対応するデータとは別のデータ・セクションに記憶される。実施形態は、二次記憶システムへの、そして特にそれからの不必要なデータ転送を除去する利点を有する。

【0024】

好適な実施形態において、データのピースは、複数の部分に分割され、複数の部分の関連の1つに対応するデータを各々が含む複数のデータ・セクションは、記憶のために二次データ記憶システムに転送される。

【0025】

この実施形態は、一次処理装置に利用可能な主メモリのサイズ、及び/またはデータ・パイプラインの幅のような二次記憶システムへのインターフェースの特性に適合可能であるよう外部化を可能とする利点を有する。

【0026】

好適な実施形態において、関連部分に対応するデータは、データのピースの関連部分を少なくとも部分的に暗号化することにより発生される。

【0027】

記憶のために二次記憶システムに転送されるデータ・セクションは、少なくとも部分的

10

20

30

40

50

に暗号化されるので、一次データ記憶ユニット、及び一次データ処理装置のプロセッサだけが、データの全体の完全な安全性を維持するために、安全環境に安置されることが必要である。一次処理装置は、制限された記憶容量を有する一次記憶ユニットだけを有することが必要であるので、データを外部的に記憶する可能性のために、かかる安全環境を提供することが一層安価でありかつ容易である。

【0028】

好ましくは、当該方法は、データのピースの各部分ごとに認証値を計算し、そして該部分に対応するデータを含むデータ・セクションに認証値を反映するデータを含めることを含む。

【0029】

このように、外部記憶されたデータの完全性が確認され得る。

【0030】

この実施形態の好適な変形態様は、入力としてさらなる部分から導出された情報を用いてデータのピースの少なくとも1つの部分のための認証値を計算することを含む。

【0031】

このように、データのピースが部分に分割されて別々のデータ・セクションに外部的に記憶される場合、データ・セクションの全体セットの完全性が確認され得る。

【0032】

好ましくは、当該方法は、各外部化された記録ごとに一次装置のデータ記憶ユニットに基準データ・オブジェクトを記憶し、独特の識別子を含めることを含み、該独特の識別子を反映するデータは、記録に属するデータのピースの部分に対応するデータを含む各データ・セクションに含まれる。

【0033】

このように、外部的に記憶されたデータのピースに対応するデータを含む種々のデータ・セクションの検索は、容易にされる。

【0034】

好ましくは、本発明の当該方法は、外部化された記録のためのバージョン・カウントを反映する情報を記憶し、そして記録を外部化する前にバージョン・カウントを増分することを含む。

【0035】

このように、記録が外部化されてしまった回数の追跡を保持することが可能である。このことは、一次記憶ユニットに記憶された記録に属するデータと、外部に記憶されたデータのピースとの同期化を可能とする。

【0036】

本発明のもう1つの態様によれば、プロセッサ、及び該プロセッサにおけるアクティブ記録を処理するよう適合された一次データ記憶ユニットを有し、該一次データ記憶ユニットにアクティブ記録に属するデータを記憶するよう構成された一次処理装置と、一次処理装置にアクセス可能な二次データ記憶システムとを含み、本発明による外部データ記憶の方法により転送されたデータのピースを記憶するよう配列されたシステムにおいて記録を内部化する（internalising）方法であって、

該方法は、記録に属するデータを、一次データ記憶ユニットにローディングするステップを含み、

前記システムは、二次データ記憶システムから記録に属するデータのピースを検索するためのインターフェースを含み、

前記方法は、さらに、記録に属するデータを用いるよう構成された応用プログラムが、記録が内部化されるべきであることを決定し、そしてインターフェースへの少なくとも1つの呼び出しを行うというステップを含む方法が提供される。

【0037】

このように、記録に属するデータを用いるよう構成された応用プログラムは、記録に属するデータのピースが、二次記憶システムから一次処理装置に転送されるべきであるとい

10

20

30

40

50

うことを決定する。一次処理装置は、二次記憶システムにデータのピースを転送することに関連した一次処理装置と同じであっても良いし、または異なったものであっても良い。従って、当該方法は、記録に属するデータが共用されるのを可能とするという利点を有する。

【0038】

本発明の好適な実施形態は、二次記憶システムからデータの1つのピースの少なくとも関連部分に対応するデータを含む少なくとも1つのデータ・セクションを受信することを含む。

【0039】

このように、データ・セクションは、1つの記録に属するデータのピースの関連部分に対応するデータを含む。1つの記録に属するデータをもう1つの記録に属するデータから分離する必要はなく、もう1つの記録に属するデータが、応用プログラムが必要とされると決定した記録に属するデータと共に不必要に転送されることもない。

【0040】

好ましくは、当該方法は、一次処理装置のデータ記憶ユニットに記憶された基準オブジェクトから記録に独特の識別子を検索するステップを含み、ここに、データ・セクションは、独特の識別子を反映する情報と共に二次データ記憶システムに記憶され、そして独特の識別子を反映する情報を含む内部化メッセージに応答して受信される。

【0041】

このように、一次処理装置は、該当データが一次データ記憶ユニットに記憶されない場合でさえ、記録の存在に気付いたままであり、それに属するデータにアクセスするための機構を有する。

【0042】

本発明の好適な実施形態は、データのピースが複数の部分を含んでいる場合に、複数の部分の関連の1つに対応するデータを各々が含む多くのデータ・セクションを受信するステップを含む。

【0043】

このように、この方法の実施形態は、内部化されている記録に属するデータのピースの部分が処理されて一次データ記憶ユニットに順次的にローディングされ得るので、制限された処理容量を有する一次処理装置、例えば制限された主メモリにおいて実行され得る。この実施形態は、また、二次データ記憶システムへのインターフェースの容量に対する何等かの制限を考慮するようにも適合されている。

【0044】

好適な実施形態は、認証値を含む少なくとも1つのデータ・セクションを受信すること、一次処理装置に記憶された情報の秘密ピースを検索すること、データのピースの少なくとも関連部分に対応するデータの少なくとも部分から各データ・セクションのための確認認証値を計算すること、情報の秘密ピースを用いること、並びに各データ・セクションごとに確認認証値と認証値とを比較することを含む。

【0045】

このように、受信されたデータ・セクションに含まれるデータが信頼できるか否かが決定され得る。確認認証値が計算されるので、それを一次処理装置に、特に、一次データ記憶ユニットに記憶する必要がない。

【0046】

好ましくは、当該方法は、外部化された記録のためのバージョン・カウントを反映する情報を含むデータ・セクションを受信すること、及び該バージョン・カウントを基準バージョン・カウントと比較することを含む。

【0047】

このことは、検索されたデータが、予想された記録のバージョンに属するデータであるということを、一次処理装置が確認することを可能とする。それは、もし他の一次処理装置がデータの外部的に記憶されたピースへのアクセスを有していたかも知れない場合には

10

20

30

40

50

、特に有用である。

【 0 0 4 8 】

本発明のもう1つの態様によれば、プロセッサ、及び該プロセッサにおけるアクティブ記録を処理するよう適合された一次データ記憶ユニットを有し、該一次データ記憶ユニットに1つのアクティブ記録に属するデータを記憶するよう構成された一次処理装置と、一次処理装置にアクセス可能な二次データ記憶システムとを含み、上述で限定された発明による外部データ記憶の方法により転送されたデータのピースを記憶するよう配列されたシステムにおいて記録の内部化を可能とする方法であって、

1つのアクティブ記録に属するデータは、一次データ記憶ユニットにロードされ、かつ記録は、記録に属するデータの少なくともピースを二次データ記憶システムから検索することにより内部化され、

10

記録を内部化する該ステップは、記録に属するデータを用いて応用プログラムにより開始される少なくとも1つの呼び出しを、二次データ記憶システムからデータのピースを検索するよう配列された応用プログラム・インターフェースにより受信することを含む方法が提供される。

【 0 0 4 9 】

この方法は、本発明による記録を内部化する方法の実施形態が行われるのを可能とするよう応用プログラム・インターフェースによって実行される。特に、それは、本発明を行うために必要とされる機能の幾つかを、多数の応用プログラムにアクセス可能な応用プログラム・インターフェースに移す。従って、この機能は、応用プログラムに含まれる必要がない。応用プログラムは、なお、どの記録がいつ内部化されるべきかを制御し、このようにして、不必要にしばしば繰り返される内部化 (internalisation) 及び外部化 (externalisation) と関連した待ち時間の多くを回避する。この実施形態は、マルチタスク能力を有した一次処理装置で使用するのに特に適している。

20

【 0 0 5 0 】

本発明は、また、外部データ記憶の方法、データを内部化する方法、マルチメディア・システムにおける記録を処理する方法、並びに一次処理装置が記録に属するデータの完全性を確認するのを許容するシステム及びコンピュータ・プログラムをも提供する。

【 0 0 5 1 】

これは、以下の方法を提供することによって達成される。すなわち、プロセッサ、及び該プロセッサにおいてアクティブ記録を処理するよう適合された一次データ記憶ユニットを有し、該一次データ記憶ユニットにアクティブ記録に属するデータを記憶するよう構成された一次処理装置と、一次処理装置にアクセス可能な二次データ記憶システムとを含むシステムにおける外部データ記憶の方法であって、該方法は、

30

アクティブ記録に属するデータを、一次データ記憶ユニットにローディングするステップ、及び

記録に属するデータの少なくともピースを記憶のために二次データ記憶システムに転送することにより記録を外部化するステップ、

を含み、該方法は、

外部化された記録のためのバージョン・カウントを反映する情報を記憶するステップ、及び

40

記録を外部化するに先立ってバージョン・カウントを増分するステップを含む方法を提供することによって達成される。

【 0 0 5 2 】

このように、外部化の後に、記録に属するデータの任意の部分、例えば、一次データ記憶ユニットに留まるデータまたは任意のデータの外部化されたピースが修正されるならば、記憶されたバージョン・カウントとの比較が行われ得て、部分がなお同期化されているか否かを決定する。

【 0 0 5 3 】

本発明は、記録が外部化された回数を反映してカウントが維持されるので、一次装置に

50

よる記録の使用の対策が得られて、限界がこの使用にセットされるのを許容するという、さらなる利点を有する。

【 0 0 5 4 】

好ましくは、当該方法は、独特の識別子、及びバージョン・カウントを反映する情報のコピーを含む、各外部化された記録ごとに、一次処理装置のデータ記憶ユニットに基準データ・オブジェクトを記憶することを含む。

【 0 0 5 5 】

このように、一次処理装置は、二次記憶システムもアクセス可能である任意の他の処理装置によって変化されることができない情報のコピーへアクセスする。

【 0 0 5 6 】

好適な実施形態は、さらに、データのピースの少なくとも関連部分に対応するデータ及びバージョン・カウントを反映する情報に対応するデータを含む少なくとも1つのデータ・セクションを二次データ記憶システムに転送することを含む。

【 0 0 5 7 】

このように、セクションにおけるデータのピースの部分のために有効なバージョン・カウントが、各セクションと共に二次記憶システムに記憶される。この実施形態は、外部に記憶される部分が記録に属するデータの全収集の同じバージョンに属するということが確認され得るような方法で、データのピースが外部に記憶された部分に分割されるのを許容するという利点を有する。特に、データ・セクションは、二次データ記憶システム内の異なった記憶ユニットに記憶されて、記録に属するデータの1つの有効な収集に再度組み立てられ得る。

【 0 0 5 8 】

好適な実施形態は、一次データ記憶ユニットにローディングした後アクティブ記録に属するデータのいずれかが変化されたか否かを決定すること、並びにアクティブ記録に属する或るデータが変化されたことを決定した後だけにバージョン・カウントを増分することを含む。

【 0 0 5 9 】

これは、バージョン・カウントが存在し得る範囲を制限する。それは、バージョン・カウントを反映する情報のコピーが一次記憶ユニットに記憶される場合に特に有利であり、その理由は、このコピーを記憶するためにより少ないメモリが留保されることが必要であるからである。

【 0 0 6 0 】

本発明のもう1つの態様によれば、プロセッサ、及び該プロセッサにおけるアクティブ記録を処理するよう適合された一次データ記憶ユニットを有し、該一次データ記憶ユニットに1つのアクティブ記録に属するデータを記憶するよう構成された一次処理装置と、一次処理装置にアクセス可能な二次データ記憶システムとを含み、本発明による外部データ記憶の最後に記載された方法のいずれか1つによる方法により転送されたデータのピースを記憶するよう配列されたシステムにおいて記録を内部化する方法であって、データのピースの少なくとも関連部分に対応するデータを含む少なくとも1つのデータ・セクションは、二次データ記憶システムから検索され、

外部化された記録のためのバージョン・カウントを反映する情報を含むデータ・セクションが受信され、そしてバージョン・カウントは基準バージョン・カウントと比較される方法が提供される。

【 0 0 6 1 】

該方法は、二次記憶システムから検索されたデータのチェックを可能とする利点を有する。それは、記録が異なった一次処理装置により外部化及び内部化されるのを許容する環境において特に有用である。記録が第1の一次処理装置によって外部化され、引き続き第2の一次処理装置により内部化されかつ外部化される場合、第1の一次処理装置は、それが最後に処理した記録のバージョンがもはや内部化のために利用可能ではないということ、を、最小の処理努力でもって決定することができる。従って、それは、二次記憶システム

10

20

30

40

50

に今や最後のバージョンに関する情報が提供されることが必要であるということを知る。

【 0 0 6 2 】

当該方法の一実施形態は、信頼のできる第三者のシステムから基準バージョン・カウントを受信することを含む。

【 0 0 6 3 】

このことは、一次処理装置における「交換 (swap)」を可能とする。第 1 の一次処理装置は記録を外部化し得る。第 2 の一次処理装置は、次に、記録を内部化してそれを処理し続けることができるように、当該方法の実施形態を実行する。それは、安全が関心事である環境において特に有用である。信頼できる第三者は、外部化される記録へのアクセスを制御する。すなわち、第 2 の一次処理装置が記録を再度外部化する場合、バージョン・カ
10
ウントは再度増分される。第 1 の一次処理装置は、信頼される第三者システムから更新されたバージョン・カウントを受信する場合、次に、記録を内部化だけをするだけである。

【 0 0 6 4 】

イベントを形成するデジタル内容の少なくとも 1 つの連続するピースへのアクセスを提供するよう適合され、かつ少なくとも 1 つの記録に含まれる情報に従ってイベントへのアクセスを制御するよう配列された条件付けアクセス・サブシステム (6 9、7 2) を含むマルチメディア・システム (5 7、6 9、7 2) において記録を処理する方法であって、
マルチメディア・システム (5 7、6 9、7 2) は、

イベントがアクセスされているときにプロセッサ (7 4) においてアクティブ記録を処理するための少なくとも 1 つの応用プログラムを走行させるよう適合された、プロセッサ (7 4) 及び一次データ記憶ユニット (7 7) を有して、一次データ記憶ユニット (7 7) にアクティブ記録に属するデータを記憶するよう構成された安全一次処理装置 (7 2) と、
20

一次処理装置 (7 2) にアクセス可能な二次データ記憶システム (5 7、6 9) と、を含む方法において、

上述の方法のいずれか 1 つを適用することにより利点が得られる。

【 0 0 6 5 】

本発明の文脈において、用語「安全」は、一次処理装置によって記憶され及び / または処理されるデータに加えられる侵襲性及び非侵襲性の攻撃に対抗する手段が、該一次処理装置に装備されるということの意味し、該手段は、ハードウェアまたはソフトウェアでの履行であって良く、もしくは両者の結合により履行されても良い。一次処理装置に改ざん防止をさせることに関連する価格及び努力は、その容量、すなわち記憶及び / または処理容量と共に増加するので、サイズ、特に、一次データ記憶ユニットのサイズを制限することが好適である。本発明は、記録に属するデータの部分またはすべてが、有利な態様で、二次記憶システム内に外部的に記憶され得るので、多くの数の異なった記録にアクセスするための容量を保持しつつ、このことを行うことができる。
30

【 0 0 6 6 】

本発明のもう 1 つの態様によれば、プロセッサ及び該プロセッサにおいてアクティブ記録を処理するよう適合された一次データ記憶ユニットを有する一次処理装置であって、一次データ記憶ユニットにアクティブ記録に属するデータを記憶するよう構成され、かつ本発明による上述した方法のいずれか 1 つを実行するよう適合された一次処理装置が提供される。
40

【 0 0 6 7 】

本発明のさらにもう 1 つの態様によれば、プロセッサ及び一次データ記憶ユニットを有する一次処理装置によって走行されるとき、該一次処理装置が本発明による上述の方法のいずれか 1 つを実行するのを可能とするコンピュータ・プログラム手段が提供される。

【 0 0 6 8 】

さて、添付図面を参照して本発明を一層詳細に説明する。

【 発明を実施するための最良の形態 】

【 0 0 6 9 】

本発明による外部データの記憶方法の一般原理を説明するために、図 1 は、本発明が適用され得るシステムの単純化された例を示す。より特定の例については、図 7 及び図 8 を参照して以下に一層詳細に説明する。

【 0 0 7 0 】

図 1 において、第 1 の処理装置 1 は、中央処理装置 (CPU) 2 と、主メモリ 3 と、一次大容量記憶装置 4 とを備える。第 1 の処理装置 1 は、例えば、サーバ (例えば、データベース・サーバ)、パーソナル・コンピュータ、個人情報機器、埋め込み処理装置、携帯電話、等として履行され得る。要するに、プロセッサ、データ記憶ユニット及び二次データ記憶ユニットにアクセスするための手段を有する任意のデータ処理装置が、本発明を履行するために適切である。履行態様に依存して、主メモリ 3 は、CPU 2 と共に単一チップ上に一体化され得る。

10

【 0 0 7 1 】

ここで説明する例において、本発明による方法は、一次大容量記憶装置 4 から二次記憶システムにデータを一時的に転送することにより、一次大容量記憶装置 4 の制限された容量を殆どを作るために用いられる。しかしながら、該方法は、主メモリ 3 のまたは CPU 2 内のキャッシュ・メモリ (図示せず) の容量を一層良く用いるために等しく良く適用されることができる。従って、ここで用いられる用語、一次データ記憶ユニットは、光学的、磁氣的及びソリッド・ステート記憶装置を含む揮発性及び非揮発性の双方のデータ記憶手段に言及することができる。

20

【 0 0 7 2 】

図 1 において、第 1 の処理装置 1 は、第 2 の処理装置 5 によって形成される二次データ記憶システムに接続される。接続は、データ・リンク 6 によって行われる。第 2 の処理装置 5 は、また、主メモリ 8 と、第 1 及び第 2 の二次大容量記憶装置 9 及び 10 を有する中央処理装置 (CPU) を備える。本発明の基本的な実施形態において、第 2 の処理装置が CPU 7 を備えることは必要条件ではないけれども、二次記憶システムが第 2 の処理装置 5 のような外部装置として履行される場合には、二次大容量記憶装置にデータを向けるために或る種類のマイクロプロセッサが存在するであろう。その最も簡単な実施形態において、本発明は、第 1 の処理装置 1 の内側の第 2 の大容量記憶装置にデータを一時的に転送することにより、一次大容量記憶装置 5 の制限された容量の殆どを簡単に作ることができた。

30

【 0 0 7 3 】

しかしながら、好適な実施形態においては、外部装置を使用する。というのは、本発明の方法は、一次処理装置が二次処理装置よりもハッキング攻撃に対して一層厳しく保証されているというシステムにおいて履行されるからである。このようなシステムにおいて、本発明による方法は、一次処理装置の容量及び / または寸法を小さく保つことができ、保護することを容易かつ安価にするという機構を提供するという点において、特に有用である。

【 0 0 7 4 】

データ・リンク 6 は、ネットワーク・リンク、例えば、イーサネット (登録商標)、IEEE 1394 (ファイヤワイヤ) リンクであって良く、もしくは、例えば、USB、SCSI、RS-232、Bluetooth、または同様の型のリンクを用いたデータ・バス・リンクであって良い。用いられるリンクの型、並びにプロトコルに属するメッセージを処理するために必要とされる処理容量に依存して、第 2 の処理装置の CPU 7 の代わりに、一層簡単なコントローラが用いられ得る。

40

【 0 0 7 5 】

第 1 の処理装置 1 は、CPU 2 によって実行される 1 つ以上の応用プログラムを走行させるよう適合される。少なくとも 1 つの応用プログラムが記録を処理するよう構成されている。本願の目的に対して、記録は、応用プログラムによって処理するように配列されたデータ項目の収集を意味すると理解される。データの配列は、それを処理する応用プログラムによって規定される。本発明は、固定された長さ及び可変の長さの双方の記録を包含

50

する。本発明によれば、CPU 2 上で実行される応用プログラムによって処理されるべき記録は、能動に為される。能動記録、すなわち任意の瞬間において第 1 の処理装置 1 上で走行されている応用プログラムによって能動にされた記録に属するすべてのデータは、少なくとも記録が能動である限りの場合に、一次大容量記憶装置 4 に記憶される。このことは、データの部分またはすべての（恐らくもはや現在のものではない）コピーが、ほかのどこかにも、例えば二次大容量記憶装置 9、10 の 1 つ上にも記憶されるということを排除するものではない。

【0076】

本発明による応用プログラムは、データの部分またはすべてを外部に記憶するか否か、すなわち、一次大容量記憶装置 4 以外の別の記憶装置上に記憶するか否かを自動的に決定するよう構成されている。このような決定が為されるルールは変わり得る。例えば、データの部分またはすべては、バックアップされ得る。しかしながら、本発明は、記録を外部化するために用いられるのが好ましく、記録に属するデータの大部分が一次大容量記憶装置 4 から移動され得てスペースを開放する。この部分、またはその回復を可能化するデータ、すなわちこの部分に対応するデータは、それぞれ外部化及び内部化と称されるプロセッサにより、記憶しそして後で取り出すために、二次大容量記憶装置 9、10 の 1 つに転送される。

【0077】

記録が外部化されるべきであるということを決定すると同時に、応用プログラムは、記録に属するデータのピースを第 2 の処理装置 5 に転送するよう配列されたインターフェースに呼び出しを行う。ここでは、インターフェースとは、二次記憶システムへの装着を支援する物理的及び論理的配列として定義される。好ましくは、さらなる応用プログラムまたはオペレーティング・システムが、第 1 の処理装置 1 上にインストールされ、該第 1 の処理装置 1 は、外部化される記録を処理する応用プログラムが呼び出しを行う応用プログラム・インターフェースを支援する。従って、第 1 の処理装置 1 のための応用プログラムの開発者は、彼ら自身、記録を外部化するための機構に正確に関心を持つ必要がない。それにも拘わらず、記録を外部化するためのロジックの部分またはすべてが応用プログラムに備えられているという実施形態を、本発明の範囲から排除するものではない。このような実施形態においては、言及されるインターフェースは、殆ど物理的インターフェース、すなわち、データ・リンクを渡ってデータを第 2 の処理装置 5 に転送するための機構である。

【0078】

本発明においては、第 1 の処理装置 1 上で走行して記録を処理する応用プログラムは、記録を外部化するためにインターフェースに呼び出しを行う。しかしながら、第 1 の処理装置上で記録を処理する応用によってそれに与えられる、記録に属するデータを用いるもう 1 つの応用も、また、呼び出しを行い、さらに、第 1 の処理装置 1 上で走行する応用プログラムによる記録の処理を終結させる。この他の応用は、第 2 の処理装置 5 上をも含む、第 1 の処理装置 1 に接続された別の処理装置上で走行していても良い。

【0079】

記録の引き続く内部化を許容するために、一次処理装置 1 の一次データ記憶装置に一次データベース（図 2）が記憶される。これは、一次大容量記憶装置 4 であるのが好ましいが、別のデータ記憶装置、例えば主メモリ 3、もしくは幾つかの他の揮発性または非揮発性メモリ・ユニットであって良い。第 1 の処理装置 1 が一次データベースを記憶する一次データ記憶ユニットは、また、周辺装置であっても良いが、一次データベースへのより早いアクセスのためには内部装置であるのが好ましいということに言及しておく。いずれの場合においても、それは、第 1 の処理装置 1 と共にされる安全な環境に備えられるのが好ましい。

【0080】

一次データベース内の一次データベース・テーブル 11 の構成が図 2 に示されている。該テーブルは、本発明の履行の例であるということに留意されたし。外部化された各記録

10

20

30

40

50

に対して少なくとも規準データ・オブジェクトがある限り、正確なデータ構造は本発明にとって重要ではない。この例においては、各外部化された記録に対し、一次データベース・テーブル 11 における行に対応する一時データベース記録 12a - 12e がある。各一時データベース記録 12 は、一次データベース記録 12 にアクセスするために用いられる独特キーまたはインデックス番号を含む、インデックス列 13 におけるフィールドを含む。インデックス列 13 における値は、各外部化された記録に対して独特である。一次データベース・テーブル 11 のバージョン番号列 14 には、各外部化された記録に対するバージョン番号が記憶される。バージョン番号は、簡単なカウンタであって良く、または、関連の外部化された記録に対するバージョン・カウントを反映した任意の他の型の情報であって良い。例えば、各々有限数の値を有し得る多くのフィールドを記録が備えている場合、バージョン番号列 14 における情報は、外部化された記録のフィールドにおける値の可能な置換の有限数の 1 つを独特に識別する情報であって良い。バージョン・カウントを反映する他の型の情報は推測可能である。

10

【0081】

本例においては、第 2 の処理装置 5 は、二次大容量記憶装置 9、10 の各々上に記憶されるデータベースに、拡張記録テーブル 15 (図 3) を維持する。示された行の各々は、拡張記録 16a - 16e に対応する。各拡張記録 16 は、外部化された記録と関連する。インデックス列 17 におけるエントリは、関連の外部化された記録に独特の識別子を反映した情報を備える。拡張記録テーブル 15 は、さらに、第 1、第 2、及び第 3 のデータ・チャンク列 18 - 21 を含む。従って、例示的な二次大容量記憶装置 9、10 における各拡張記録は、3 つのデータ・チャンクを含み得る。外部化された記録に対する拡張記録 16 における各データ・チャンクは、外部化された記録に属するデータのピースの少なくとも関連部分に対応するデータを含む。対応とは、データのピースの関連部分が、外部化された記録におけるデータから完全に回復され得るということを意味する。従って、データ・チャンクにおけるデータは、外部化された記録に属するデータのピースの関連部分の暗号化された、符号化されたまたは圧縮されたバージョンであって良い。認証ストリングが各データと共に記憶されるのが好ましい。拡張記録テーブルは、さらに、外部化された記録のためのバージョン・カウントを反映する情報が記憶されたバージョン番号列 21 を含む。一次データベース・テーブル 11 (図 2) のバージョン番号列 14 におけるエントリと関連させて上述したことは、また、図 3 に示されたバージョン番号列 21 におけるエントリに対しても当て嵌まる。代替的な履行において、第 1、第 2 及び第 3 のデータ・セクション列 18 - 20 の 1 つにおける各データ・チャンクは、当該データ・チャンクだけに対して有効なバージョン・カウントを反映する別の情報を備えるかもしくは該情報で記憶されて良い。

20

30

【0082】

記録が、本発明を用いて第 1 の処理装置 1 上で走行している応用プログラムによって創成されるとき、第 1 の処理装置 1 は、図 4 に示されるステップを通して行く。第 1 のステップ 22 において、バージョン・カウントが初期設定される。例えば、順次的な番号が用いられる場合、バージョン・カウンタは、値ゼロにセットされる、すなわち、マイナス 1 からゼロに増分される。応用プログラムは、次に、記録を能動にし、それを通常に処理することに進む。処理中、応用プログラムによって修正された記録に属するデータは、一次大容量記憶装置 4 に記憶される。或る点において、応用プログラムは、記録がもう処理されないであろうということ、または、記録を外部化するためのもう 1 つの理由が存在するということを決意し得る。従って、それは、インターフェースに呼び出しを行うことによって、記録の外部化を開始するであろう。述べたように、これは、第 1 の処理装置 1 のオペレーティング・システムの部分として与えられる応用プログラム・インターフェースであり得るか、またはもう 1 つの応用プログラムによるものであり得る。

40

【0083】

少なくとも CPU 2、主メモリ 3 及び一次大容量記憶装置 4 は安全環境の部分であり、記録に属するデータが保護されるべきであると仮定している。従って、第 2 のステップ 2

50

3において、記録に属するデータが暗号化され、少なくとも1つの認証ストリングが該データのために計算される。さらなるステップ24において、一次記録は、一次大容量記憶装置4における一次データベース・テーブル11に書込まれる。このことは、インデックス列13における対応のエントリに外部化されている記録に独特の識別子を反映する情報を入れることを伴う。さらに、バージョン・カウントがバージョン番号列14におけるエントリに書込まれる。従って、基準データ・オブジェクトが、外部化された記録のための一次大容量記憶装置4に記憶され、該基準データ・オブジェクトは、独特の識別子と、バージョン・カウントを反映する情報のコピーとを含む。

【0084】

次に、記録に属するデータの暗号化されたピースは、ステップ25において、認証ストリング及びバージョン・カウントを反映する情報と一緒に、第2の処理装置5に転送される。第2の処理装置5は、拡張記録テーブル15における転送されたデータ・セクションの内容を記憶する。

【0085】

本発明によれば、外部化された記録を用いる応用プログラムは、また、記録を再度内部化することを自発的に決定し得る。内部化プロセスの実施形態が図5に示されている。従って、或る点において、記録に属するデータを用いる、すなわち用いるように構成された応用プログラムは、記録が内部化されるべきであることを決定する。応用プログラムは、二次記憶システムに対するインターフェースに呼び出しを行う。二次記憶システムに対するインターフェースの部分であるソフトウェア、例えば応用プログラム・インターフェースは、メッセージが第2の処理装置5に送られるのを確実にして、外部化された記録に属するデータに対応するデータを含むデータ・セクションを要求する。メッセージは、外部化された記録に独特の識別子を反映する情報を少なくとも含む。この情報は、一次データベース・テーブル11のインデックス列13における関連のエントリから検索される。インターフェースは、外部に記憶されたデータのピースの少なくとも関連部分に対応するデータを含む少なくとも1つのデータ・セクションが、ステップ26において検索されるのを確実にする。検索されたもしくは取り出されたデータ・セクションは、バージョン・カウントを反映する情報を含む。この情報は、拡張記録テーブル15のバージョン番号列21における関連エントリから得られる。ステップ27において、第1の処理装置1は、秘密の暗号キーを用いて、検索されたデータ・セクションにおけるデータのピースの暗号化された部分を解読する。それは、次に、解読されたデータから検証認証ストリングを計算する。検証認証ストリングは、ステップ28において、検索されたデータ・セクションに含まれた認証ストリングと比較される。両者が一致すれば、バージョン・カウントが、検索されたデータ・セクションに含まれる情報から導出され、一次データベース・テーブル11のバージョン番号列14におけるエントリから導出されたバージョン・カウントと比較される。両者が一致すれば、データの解読されたピースは、今内部化された記録を組み立てるために用いられる。内部化された記録は、応用プログラムによる使用のために、一次大容量記憶装置4内に記憶される。

【0086】

第1の処理装置1上で走行している応用プログラムは、実際、記録に属するデータを修正する(ステップ29)と仮定している。修正の後、それは、再度、記録が外部化されるべきであるということを決して得る。この場合において、バージョン・カウントは、ステップ30において、更新され、すなわち、増分される。記録に属するデータのピースは暗号化され、そしてステップ31において、そのための認証ストリングが計算される。次に、一次データベース・テーブル11における一次記録が再書き込みされ、すなわち、増分されたバージョン・カウントを反映する情報が、バージョン番号列14における対応のエントリに書き込まれる。データの暗号化されたピース、認証ストリング、及び更新されたバージョン・カウントを反映する情報のコピー、を含むデータ・セクションが、第2の処理装置5に転送され、そこで、拡張記録テーブル15における対応の拡張記録16が更新され、もしくはそれが消去されていたならば再書き込みされる。

10

20

30

40

50

【 0 0 8 7 】

本発明の好適な実施形態は、CPU 2 及び / または主メモリ 3 及び / またはデータ・リンク 6 の特性を考慮するということを述べておく。これは図 6 に示されている。記録に属するデータ 3 4 のピースの部分は、検索されたデータ・セクションから転送されるまたは検索されるべきデータ・セクションに含めるよう処理されるが、それは主メモリ 3 に保持される。従って、CPU 2 または主メモリ 3 の容量は、境界 (bound) を部分のサイズに設定し得、その境界の上では、内部化及び外部化が第 1 の処理装置 1 を受け入れがたいほどゆっくりさせるであろう。データのピースの部分のサイズに対するもう 1 つの制限は、暗号化された部分、認証ストリング及びバージョン・カウント及びインデックス情報を含む、結果のデータ・セクションのサイズである。上述の制約の最大の制限を考慮して、第 1 の処理装置 1 は、外部化されるべき記録に属するデータ 3 4 のピースを、第 1 のステップ 3 8 において、複数の部分 3 5 - 3 7 に分割する。この場合、第 1、第 2 及び第 3 の部分 3 5 - 3 7 がある。部分 3 5 - 3 7 への分割は、記録を処理する応用プログラムによって、または応用プログラムによって呼び出された応用プログラム・インターフェースに属するモジュールを実行することによって行なわれ得る。引き続くステップ 3 9 において、部分 3 5 - 3 7 の各々は、一次大容量記憶装置 4 及び CPU 2 及び主メモリ 3 もまたその部分である安全環境の内側に記憶された、秘密暗号化キー 4 0 を用いて別々に暗号化される。第 1 のデータ・チャンク 4 1 は、外部化されている記録に属するデータ 3 4 のピースの第 1 の部分 3 5 に対応し、第 2 のデータ・チャンク 4 2 は、第 2 の部分 3 6 に対応し、そして第 3 のデータ・チャンク 4 3 は第 3 の部分 3 7 に対応する。

10

20

【 0 0 8 8 】

次のステップ 4 4 において、第 1 の認証ストリング 4 5 は、入力としての第 1 のデータ・チャンク 4 1、並びに秘密認証キー 4 6 を用いて、データ 3 4 のピースの第 1 の部分 3 5 に対して計算される。秘密認証キー 4 6 も、一次大容量記憶装置 4 及び CPU 2 及び主メモリ 3 もまたその部分である安全環境の内側に記憶されている。後続のステップ 4 7 において、第 1 のデータ・セクション 4 8 が創成される。第 1 のデータ・セクション 4 8 は、第 1 のデータ・チャンク 4 1、第 1 の認証ストリング 4 5、外部化された記録のための一次データベース・テーブル 1 1 のインデックス列 1 3 におけるエントリに記憶されたインデックスの値に対応する情報、及び第 1 のデータ・セクション 4 8 がデータ 3 4 のピースを構成する部分 3 5 - 3 7 のシーケンスにおける第 1 の部分 3 5 と関連しているという事実を反映する情報を含む。この第 1 のデータ・セクション 4 8 は、次に、記憶のために第 2 の処理装置 5 に転送される。

30

【 0 0 8 9 】

同時に、第 2 の認証ストリング 4 9 は、ステップ 5 0 において計算される。第 2 の認証ストリング 4 9 は、第 2 のデータ・チャンク 4 2 及び第 1 の認証ストリング 4 5 から計算される。これは、例えば、最初に第 2 のデータ・チャンク 4 2 を第 1 の認証ストリング 4 5 と連結させ、次に、その結果を、ステップ 4 4 で用いられたのと同じ、認証キー 4 6 を用いた認証アルゴリズムに従属させることによって行われ得る。

【 0 0 9 0 】

ステップ 5 1 において、第 2 のデータ・セクション 5 2 が創成される。ステップ 5 1 はステップ 5 0 に対応する。従って、第 2 のデータ・セクション 5 2 は、第 2 のデータ・チャンク 4 2、第 2 の認証ストリング 4 9、及び外部化された記録に独特の識別子を反映する情報、並びに第 2 のデータ・セクション 5 2 がデータ 3 4 のピースから形成される部分 3 5 - 3 7 のシーケンスにおける第 2 の部分 3 6 と関連しているという事実を反映する情報を含む。

40

【 0 0 9 1 】

ステップ 5 3 において、第 3 の認証ストリング 5 3 が、入力としての第 2 の認証ストリング 4 9、並びに認証キー 4 6 及び第 3 のデータ・チャンク 4 3 を用いて計算される。ステップ 5 3 は、実質的にステップ 5 0 に対応する。

【 0 0 9 2 】

50

ステップ55において、第3のデータ・セクション56が創成されて、第2の処理装置5に転送される。第1及び第2のデータ・セクション48、52と同様に、第3のデータ・セクション56は、第3のデータ・チャンク43、第3の認証ストリング54、及び外部化された記録に独特の識別子を反映する情報、並びに第3のデータ・セクション56が、データ34のピースから形成される部分のシーケンスにおける第3の部分37と関連しているという事実を反映する情報を含む。

【0093】

本発明の方法は、データ34のピースが属する記録以外の記録に属するデータのピースにも同時に適用され得るということを述べておく。しかしながら、1つの記録に属するデータ34のピースの部分35 - 37と関連するデータ・セクション48、52、56は、
10
もう1つの記録に属するデータのピースの部分と関連するデータ・チャンクを含まない。このことは、第1、第2及び第3のデータ・セクション48、52、56が、データ・リンク6に適切なサイズのままであるということを確認にする。それは、また、第2の処理装置5による効率的な処理をも確認にする。特に、記録が再度内部化されるとき、第1、第2及び第3のデータ・セクション48、52、56の正確なコピーが検索される。データの不必要な転送を避けるために、1つの記録のために創成されたデータ・セクションをもう1つの記録のために創成されたデータ・セクションから分離することが有利である。

【0094】

図7は、本発明の応用に良く適している、記録が処理されるシステムの特定の例を示す。示されたシステムは、デジタル内容の少なくとも1つの連続したピースへのアクセスを
20
提供するように適合されたマルチメディア・システムであり、デジタル内容へのアクセスを制御するための条件付きアクセス・サブシステムを備えている。特に、図7は、内容データの分配器からダウンロードされた、もしくは該分配器から同報通信で受信された内容データを記録し及び再生するための個人ビデオ記録器57を示す。

【0095】

個人ビデオ記録器は、特定の搬送周波数に同調させるためのチューナ58を備える。それは、さらに、デジタル内容を担持する1つ以上の基本ストリームを含む輸送ストリームを検索するための復調器59を備える。それらは、例えば、MPEG-2基本ストリームまたはMPEG-4アクセス・ユニットのストリームであって良い。基本ストリームは、この目的のために主メモリ61へのアクセスを有するマルチメディア・プロセッサ60に
30
よって処理される。マルチメディア・プロセッサ60は、例えばI²Cバスであるシステム・バス62に接続される。マルチメディア・プロセッサ60は、さらに、ビデオ・エンコーダ63及びオーディオ・デジタル・アナログ・コンバータ(DAC)64に接続される。従って、個人ビデオ記録器は、適切な出力を通してテレビジョンのような再生装置に利用可能なアナログ・ビデオ及びオーディオ信号を作ることができる。もちろん、代替的な実施形態において、個人ビデオ記録器は、また、例えばイーサネット(登録商標)またはIEEE 1394ホーム・ネットワークを介して1つ以上のホーム・ネットワーク・エンド装置に運ばれる(保護されない)MPEG-2符合化されたストリームの形態で利用可能な出力を作るためのエンコーダを備えることもできる。

【0096】

インターフェース・コントローラ65は、また、システム・バス62にも接続される。インターフェース・コントローラ65は、ユーザから、個人ビデオ記録器57の動作を制御するマルチメディア・プロセッサ60への指令を中継し、そして任意選択的にユーザにフィードバック情報を提供し得る。例えば、インターフェース・コントローラは、リモート・コントロール・ユニット(図示せず)からの指令を受け入れるための赤外線ポートを制御することができるか、または個人ビデオ記録器57のフロント・パネル・インターフェイスを制御することができる。
40

【0097】

個人ビデオ記録器57は、さらに、システム・バス62に接続され、かつ光ディスク・ドライバ67及びハード・ディスク・ドライバ68に接続されたディスク・コントローラ
50

66を備える。光ディスク・ドライバ67及びハード・ディスク・ドライバ68は、本発明による方法で用いるための二次データ記憶システムに備えられた大容量記憶ユニットの単に代表として考慮されるべきである。

【0098】

条件付きアクセス・サブシステムは、条件付きアクセス・モジュール70に及びから通信を向けるためのプロセッサ71を含む条件付きアクセス・モジュール(CAM)70を備える。CAM73は、さらに、暗号の共同プロセッサ(co-processor)72、暗号化及び/または解読化動作を行なうための専用のデジタル信号プロセッサを含む。このようなCAM70の例は、デジタル・ビデオ・ブロードキャスト(DVB)の履行から既知であり、それにおいて、CAM70は、個人ビデオ記録器57が特定の例である集積化された受信器レコーダと、共通のインターフェース(CI)を通して通信する。これらの既知の履行において、条件付きアクセス・モジュール70は、PCMCIAカードの形状に来る。

10

【0099】

条件付きアクセス・サブシステムは、さらに、スマート・カード集積回路(IC)73を担持しているスマート・カード72を備える。スマート・カード72は、ISO 7816-2規格に適合しているのが好ましい。スマート・カード72は、スマート・カード上の接点パッド(図示せず)及びCAM70における接点ピン(図示せず)を備えた物理的相互接続システムにより、そして通信プロトコルを履行する1つ以上のソフトウェア・モジュールにより、CAM70にインターフェースし、かつそれを通して個人ビデオ記録器57にインターフェースする。

20

【0100】

図8は、スマート・カードIC73が中央処理装置(CPU)74を含むことを示す。それは、さらに、3つの型のメモリ・モジュール、すなわちマスク・リード・オンリ・メモリ(マスクROM)75、ランダム・アクセス・メモリ(RAM)76、及び電子的に消去可能のプログラマブル・リード・オンリ・メモリ(EEPROM)77を含む。もちろん、スマート・カードIC73は、また、CAM70へのインターフェースの部分としての入力/出力(I/O)ポート78をも備える。スマート・カードIC73の代替的な実施形態は、EEPROM77の代わりに、強誘電性ランダム・アクセス・メモリを備えていても良い。

30

【0101】

マスクROM75は、不揮発性メモリである。スマート・カード72のオペレーティング・システムは、マスクROM75内に記憶される。適切なオペレーティング・システムの例は、MULTOS、Java(登録商標)card及びWindows(登録商標)cardである。さらに、1つ以上の秘密キーがマスクROM75内に記憶されても良い。RAM76は、メモリの作業空間を形成する。RAM76は、揮発性メモリであり、そしてスマート・カードIC72への電力が除去されたとき、すべてのデータは喪失される。EEPROM77は、ダイナミック・アプリケーション・データを記憶するための不揮発性記憶メモリを表す。

【0102】

40

スマート・カードIC73内に備えられた3つの型のメモリの内、RAM76が一般に最も高価であり、それに続いて、EEPROM77及びマスクROM75がこの順番で続く。結果として、特により高価な型のメモリの量を制限するように保つことが有利である。スマート・カード72の一次データ記憶ユニット、すなわちEEPROM77内に記憶されたダイナミック・アプリケーション・データ内に備えられた記録を内部化する及び外部化することによって、スマート・カード72は、制限された容量のEEPROM77でもって行なわせ得る。内部化された及び外部化された記録に属するデータのピースを部分に分割することによって、本発明による方法の部分として、スマート・カードIC73は、制限されたサイズのRAM76及び制限された容量のI/Oポート78でもって管理することができる。

50

【 0 1 0 3 】

図 7 に示されたマルチメディア・システムが代表的に用いられる同報通信システムは、すべての加入者の詳細が保持されている加入者管理システム（SMS）を備える。加入者が可能化されているチャンネル及びイベント、加入者の支払い状況、加入者のスマート・カード 7 2 が活性化しているかいないか、のような情報及び他の情報が SMS 上に保持される。イベントとは、デジタル内容の連続したピースとして、例えば、双方とも条件付けアクセスに従属しかつ関連のイベント情報を有する DVB-MPEG-2 サービスのピースとして定義される。イベントは、キーとして 1 つ以上の制御ワードでスクランプリング・アルゴリズムにスクランブルされる。SMS から、払込金（サブスクリプション）の支払いのための請求書が送られる。SMS は、加入者に配分されたスマート・カード 7 2 を、条件付けアクセス（CA）システムを介してそれらに指令を送ることによって制御する。CA システムは、これらの指令をスマート・カード 7 2 のための正しいフォーマットに変換し、該指令を搬送ストリームに挿入する。CA システムのもう 1 つの役目は、加入者に同報通信されるときにイベントがスクランブルされる制御ワードを暗号化することである。これらの暗号化された制御ワードは、資格（エンタイトルメント）制御メッセージ（ECM）としてイベントを形成する内容と一緒に送信される。

10

【 0 1 0 4 】

同報通信において起こる各イベントおよび申し込み（オファー）の内容は、スケジューリング・システムによってスケジュールされる。該内容は、内容サーバによって、符号化され / 圧縮される。内容サーバ及び CA システムからのフォーマット化されたデータは、搬送ストリームに多重化され、該搬送ストリームは、次に、適切な同報通信ネットワーク（すなわち、衛星、ケーブル、地上局、インターネット、等）のために変調される。

20

【 0 1 0 5 】

個人ビデオ記録器 5 7 は、搬送ストリームを回収もしくは再生するために、チューナ 5 8 及び復調器 5 9 を用いる。スクランブルされている搬送ストリームは、マルチメディア・プロセッサ 6 0 により条件付けアクセス・モジュール 7 0 に経路付けられる。条件付けアクセス・サブシステムは、キー階層を用いて搬送ストリームをスクランブル解除（デスクランブル）する。スマート・カード 7 2 内に、例えばマスク ROM 7 5 内に記憶されているのは、Xkey として知られているスマート・カード 7 2 に特有のキーである。幾つかの代替的なシステムにおいては、Xキーの階層があっても良く、その内の高い方のレベルの階層はグループ・キーと呼ばれ、加入者のグループに割り当てられる。単純化のために、ここの説明では 1 つのレベルだけを仮定する。

30

【 0 1 0 6 】

マルチメディア・システムは、イベント管理システム（EMS）を履行する 1 つ以上のソフトウェア・モジュールを備え、その内の少なくとも幾つかがスマート・カード 7 2 にインストールされる（他は、個人ビデオ記録器 5 7 または CAM 7 0 にインストールされ得る）。イベント管理システムは、イベントへのアクセスを制御するために用いられる情報を含む記録を処理する、スマート・カード 7 2 上で走行するアプリケーションを備える。これらの記録は、セッション記録及びイベント記録を含む。イベント記録及びセッション記録が処理されている間、それらは活性であり、かつ EEPROM 7 7 に記憶される。イベント記録及びセッション記録の双方は、記録に属するデータの少なくとも 1 つのピースを、二次記憶システムにおける記憶装置に、例えば個人ビデオ記録器 5 7 におけるハード・ディスク・ドライブ 6 8 に転送することにより外部化されることができる。

40

【 0 1 0 7 】

例示的な実施形態において、イベント記録は、以下のフィールド、すなわち、アクティブ・フラッグ、変化されるフラッグ、バージョン番号、記録識別、再生カウント、及びコピーの番号のカウントを含む。アクティブ・フラッグは、イベント記録がアクティブであるすなわち活性化である各時間毎にセットされる。イベント記録は、少なくともイベントが記録され、コピーされまたは再生されるときに、アクティブであるすなわち活性化している。イベント記録がアクティブであるとき、それは、スマート・カードの CPU 7 4 に

50

よって処理され、記録に属するデータは、EEPROM 77に記憶される。イベント記録の処理の間に、イベント記録に属するデータのいずれかに変化が為されたならば、変化されたフラッグがセットされる。変化されたフラッグを有することの長所は、不必要な外部化が阻止され得るということである。好適な実施形態において、イベント記録を外部化するための指令が受信されると、最初に、変化されたフラッグについてチェックが為される。もしそれがセットされていないならば、個人ビデオ記録器 57に記憶されたコピーがまだ正確ではないので、外部化は必要ではない。イベント記録の各外部化に先立ってバージョン番号が増分される。記録の識別は、イベント記録が、スマート・カード 72上の応用プログラム・インターフェースに対して及びそれによって為される呼び出し内に識別されるのを許容する。再生カウント及びコピーの番号のカウントは、関連のイベントへのアクセスを提供するためにイベント記録がアクティブにされるごとに増分される、再生カウントを反映する情報の双方の型である。このことは、例えば、イベントのコピーを行うために、それをスクランブル解除しかつ復号するために、それを光ディスク・ドライブ 67またはハード・ディスク・ドライブ 68等に挿入された光ディスクに記録するために、イベントへのアクセスが必要とされるときはいつも行われる。

【0108】

セッション記録は、エンタイトルメント情報及びプログラム・キー(P-Keys)を含む。P-Keysは、受信されたECMに含まれる暗号化された制御ワードを解読するために必要とされ、個人ビデオ記録器 57によって、スクランブルされた搬送ストリームの部分として記録され得る。イベントのためのP-Keys及びエンタイトルメント情報は、イベントのための支払いを行うことによって得られ、その上で、放送会社のCAシステムは、スマート・カード 72のX-Keysの下で暗号化されたP-Keys及びエンタイトルメント情報を含む1つ以上のエンタイトルメント管理メッセージ(EMM)を送信する。スマート・カード 72は、EMMからP-Keys及びエンタイトルメント情報を検索し、それらをセッション記録に加える。記録を行っているセッションごとに、すなわち、ハード・ディスク・ドライブ 68上にまたは光ディスク・ドライブ 67のディスク上に内容データが記録される各連続する期間ごとに、セッション記録が存在する。各セッション記録は、1つ以上のイベント記録と連結し、従って、これらのイベント記録が関連するイベントを関連する。イベントの1つへのアクセスは、セッション記録がアクティブである時間である、すなわちセッション記録に属するデータがEEPROM 77内に存在する時間である、観察セッションの間に提供される。イベント記録は、また、イベントの再生の間、アクティブである。

【0109】

イベント及びセッション記録の外部化及び後での内部化を可能とするために、スマート・カード 72は、EMSを履行してこのようにイベント及びセッション記録を用いるアプリケーションからのメッセージを受信しかつ処理するよう配列された応用プログラム・インターフェースを備える。イベントがセッション中に記録されており、イベントにアクセスするために必要とされるP-Keysが関連のセッション記録に記憶されていると仮定すると、記録を制御してこのようにイベント及びセッション記録を用いるアプリケーションは、記録が完了してしまい再生が直ちには必要とされない場合に、記録の外部化を履行するスマート・カード APIへの外部化呼び出しを行う。以下の説明は、セッション記録の外部化が同様の方法で行われるという理解において、イベント記録の外部化に焦点を合わせる。

【0110】

一実施形態において、APIは、記録に属するデータのすべてまたはそのサブセットを含み得る、記録に属するデータのピースを、一連の連続する部分に分割する。各部分は、個人ビデオ記録器 57のハード・ディスク・ドライブ 68及びEEPROM 77間のインターフェースの最大処理容量に従ってサイズが決められる。最大処理容量は、RAM 76、中央処理装置 74、I/Oポート 78、プロセッサ 70、CAM 69及び個人ビデオ記録器 57間のPCMCIAインターフェース、のサイズによって、または特定の履行に依

存して、システム・バス 62 のサイズによって決定され得る。

【0111】

引き続いて、API は、各部分ごとに外部化メッセージを受信し、各外部化メッセージは、転送されるべきデータのピースの少なくとも関連部分に対応するデータを含むデータ・セクションを転送するための要求を表す。API は、図 6 と関連して概要を記述した方法を用いてデータ・セクションを発生する。すなわち、イベント記録に属するデータのピースの各部分は暗号化され、そしてそれに対して認証値が計算される。データのピースの各部分ごとに、別々のデータ・セクションが創成され、該別々のデータ・セクションは、計算された認証値、データのピースの暗号化された部分、データのピースを連続する部分に分割することにより創成された部分のシーケンスにおける部分の位置を含む。さらに、セクションは、バージョン番号を反映する情報を含む。

10

【0112】

API は、各データ・セクションごとに別々の外部化メッセージを受信する。図 6 に示された方法を用いて創成されたデータ・セクションは、各々関連の外部化メッセージに回答して、1 つずつ戻される。これらの外部化メッセージは、イベント記録識別に対応する情報、及び部分のシーケンスにおけるデータのピースの関連部分の位置によってデータ・セクションを識別する情報を備える。任意選択的には、API は、最初に受信された呼び出しに回答して、シーケンス内にいかに多くの部分が存在するかを表す情報を戻しても良い。

【0113】

20

最後のデータ・セクションが転送されてしまった後、アプリケーションは確認要求を送る。正しい外部化が確認されたならば、EEPROM 77 内に保持された記録に属するデータのコピーにおける変化されたフラッグは、リセットされる。そのときだけ、記録は不活性もしくはインアクティブにされ得、外部記憶のために転送された記録に属するデータのピースは、EEPROM 77 から削除され得る。しかしながら、基準データ・オブジェクトは、各外部化された記録ごとに EEPROM 77 内に保持される。基準データ・オブジェクトは、記録識別及びバージョン番号を含む。

【0114】

例えば、関連のイベントの再生を可能化するために、イベント記録が再度内部化される時、スマート・カード API は、イベント記録に属するデータを用いてアプリケーションから呼び出しを受信する。API は、次に、ハード・ディスク・ドライブ 68 に記憶されたデータ・セクションを検索する。再度、データ・セクションは、別々に検索されて処理される。各データ・セクションが、シーケンス内の良く定義された位置を有して記録に属するデータのピースの部分に対応するデータを含む場合、データ・セクションは順番に検索される。従って、シーケンス内の最初の部分に対応するデータを含むデータ・セクションが最初に検索される。このことは、データ・セクションのすべてをまずバッファリングしなければならないという必要性無しで、各セクションごとに基準認証値を計算することができるようにするために必要である。最初のセクションのための基準認証値だけが、他のデータ・セクションの 1 つ以上に対して計算される基準認証値を用いることなく計算されることができる。計算された基準認証値の使用は、基準認証値を記憶するための必要性を除去するということに留意されたい。認証キーだけが記憶されることが必要である。認証キーは、EEPROM 77 よりも安価であるマスク ROM 75 に記憶され得る。代替的には、スマート・カード 72 の寿命の間に認証キーの変化を許容するために EEPROM 77 に記憶されても良い。

30

40

【0115】

データ・セクションは、スマート・カード 72 に記憶された暗号化キーを用いて解読される（対称アルゴリズムが用いられるということを仮定している）。次に、データ・セクションが含まれたバージョン番号が計算された基準認証値と比較され、イベント記録のバージョン番号は、EEPROM 77 に記憶された基準データ・オブジェクトに記憶されたバージョン番号と比較される。双方が正しいならば、プロセスは、引き続くデータ・セク

50

ションの各々ごとに反復され、イベント記録に属するデータのピースは、EEPROM 77に再組み立てされる。その後、イベント記録は、活性化されて、それからデータ検索され得、条件付けアクセス・サブシステムが、再生、コピー、またはハード・ディスク・ドライブ 68 に記憶されたイベントの他の使用を制御するのを許容する。

【0116】

イベント記録に属するデータが暗号化された形態で外部的に記憶されるので、例えば、セッション記録におけるエンタイトルメント情報に従って許容される以上の観察を可能とするために、ハッカーが再生カウントを下方に修正することは困難である。たとえハッカーが暗号化キーを推論したとしても、次に、下方に修正された再生カウントに対応する情報を含むデータ・セクションのための新しい認証値を計算するために、認証キーが必要となるであろう。連鎖が使用されるので、イベント記録と関連した他のすべてのデータ・セクションのための認証値も必要であろう。一層早期のデータ・セクションのコピーを簡単に作ることは可能ではなく、その理由は、そのバージョン番号が、スマート・カード 72 の EEPROM 77 における基準データ・オブジェクトに記憶されたバージョン番号と整合しないからであり、それ故、このように一層早期のデータ・セクションは、イベント記録の上首尾の内部化には導かないであろう。

【0117】

スマート・カード 72 の EEPROM 77 内に留まる基準データ・オブジェクト内に、及びハード・ディスク・ドライブ 68 に転送されるデータ・セクション内に、バージョン番号を含めることは、第 1 のスマート・カードを第 2 のスマート・カードに取り替えるためのプロセスを履行するのを可能とする。第 2 のスマート・カードには、個人ビデオ記録器 57 にデータを同報通信する CA システムのような、信頼できる第三者からであるのが好ましい、第 1 のスマート・カードにおける基準データ・オブジェクト内のデータに対応するデータが提供される。第 2 のスマート・カードは、次に、提供されたデータを用いて記録を内部化することができる。それが、引き続いて再度、記録を内部化するとき、バージョン番号が増分される。従って、第 1 のスマート・カードは、もはや、記録を内部化しないであろう。というのは、それは、記録のための先のバージョン番号でもって基準データ・オブジェクトを記憶しつつあるからである。もちろん、第 2 のスマート・カードには、暗号化及び認証キー、並びに基準データ・オブジェクトが提供されるべきである。

【0118】

本発明は、上述の実施形態に制限されるものではなく、添付の特許請求の範囲内で変化し得る。例えば、挿入されたスマート・カード 72 を有した条件付アクセス・モジュール 69 及び個人ビデオ記録器 57 を備えたシステムが、本発明の適用に同様に良く適した同様のマルチメディア・システムを代表する。これは、個人ビデオ記録器の代わりのセット・トップ・ボックス、条件付けアクセスの方法によって保護されたデジタル内容を受信するための関連の周辺機器ハードウェアを有するパーソナル・コンピュータ、もしくはアナログ信号を受信するよう配列された個人ビデオ記録器を含むシステムを含む。

【図面の簡単な説明】

【0119】

【図 1】本発明が意図されたシステムの型を示す概観図である。

【図 2】本発明の変形例における一次処理装置によって維持されるデータベースを示す概略図である。

【図 3】図 2 の変形例における二次記憶システムに記憶されたデータベースを示す概略図である。

【図 4】記録の創成を示すフローチャート図である。

【図 5】一次処理装置による記録の修正を示すフローチャート図である。

【図 6】記録の外部化における幾つかのステップを示すフローチャート図である。

【図 7】本発明が履行されたマルチメディア・システムの例を示す図である。

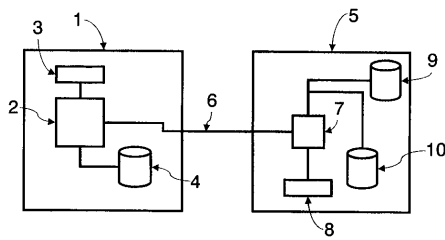
【図 8】図 1 に示される一次処理装置の基本構成の例を示す図である。

【符号の説明】

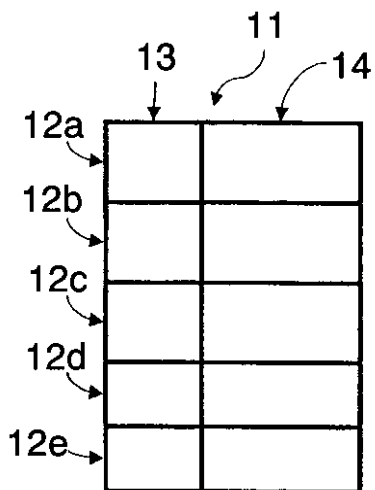
【 0 1 2 0 】

1・・・第1の処理装置、2・・・中央処理装置（CPU）、3・・・主メモリ、4・・・一次大容量記憶装置、5・・・第2の処理装置、6・・・データ・リンク、7・・・CPU、8・・・主メモリ、9・・・第1の二次大容量記憶装置、10・・・第2の二次大容量記憶装置。

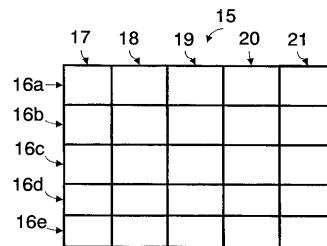
【 図 1 】



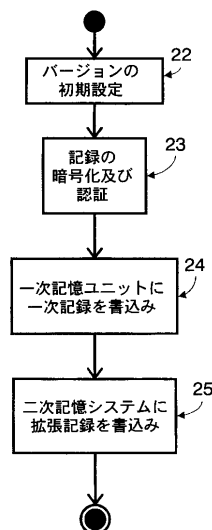
【 図 2 】



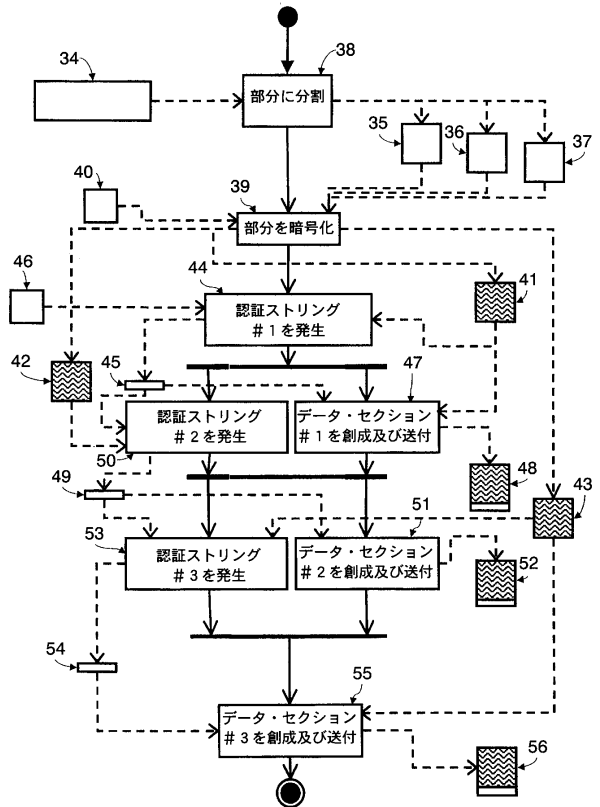
【 図 3 】



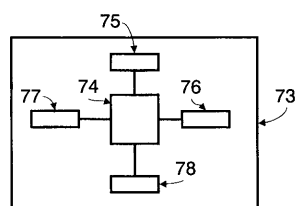
【 図 4 】



【 図 6 】



【 図 8 】



フロントページの続き

- (72)発明者 ジェレルド・ヨーハン・デッカー
オランダ・2151・EB・ニーウ・ヴェネップ・ラーン・ヴァン・ルーフェステイン・30
- (72)発明者 アルベルト・ヤン・ボスハ
オランダ・2134・VC・フーフドドルプ・ルーケンボス・99
- (72)発明者 アントニウス・ヨハネス・ペトラス・マリア・ヴァン・デ・ヴェン
オランダ・3111・PG・スキーダム・ノールドヴェスト・141

審査官 児玉 崇晶

- (56)参考文献 特表2003-530646(JP,A)
特表2001-508893(JP,A)
特開平01-213711(JP,A)
特開平10-222425(JP,A)
特開平07-152643(JP,A)
特開平02-005158(JP,A)
特表平11-508117(JP,A)
特開平05-165718(JP,A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| G06F | 21/24 |
| G09C | 1/00 |