(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2003/065225

発行日　平成17年5月26日(2005.5.26)

(43)国際公開日　平成15年8月7日(2003.8.7)

(51)Int.Cl.[7]	F I		
G06F 12/14	G06F	12/14	560E
G06F 12/16	G06F	12/16	320B
	G06F	12/16	320M

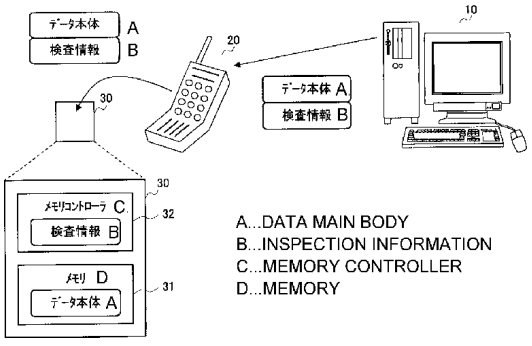
審査請求 未請求　予備審査請求 未請求　（全 27 頁）

出願番号	特願2003-564748 (P2003-564748)
(21)国際出願番号	PCT/JP2003/000500
(22)国際出願日	平成15年1月22日(2003.1.22)
(31)優先権主張番号	特願2002-23704 (P2002-23704)
(32)優先日	平成14年1月31日(2002.1.31)
(33)優先権主張国	日本国(JP)
(81)指定国	EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),CN,JP,KR,US

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　中西　良明
東京都杉並区松ノ木２－４－１０－３０５
(72)発明者　佐々木　理
東京都大田区東六郷２－２０－５－６２０
(72)発明者　高木　佳彦
東京都大田区東六郷２－２０－５－５０６

(54)【発明の名称】メモリデバイス、端末装置及びデータ修復システム

(57)【要約】
データとデータの破損を検査するための検査情報とを管理するサーバ１０と、サーバ１０から前記データと検査情報とを取得する端末装置２０と、端末装置２０が取得したデータを非耐タンパ性のメモリ領域３１に格納し、検査情報を耐タンパ性のメモリ領域３２に格納するメモリデバイス３０とで構成する。メモリデバイス３０は、検査情報を用いてデータ破損が生じているデータを検出し、端末装置２０は、検出されたデータをサーバ１０から取得し、メモリデバイス３０は、端末装置２０が取得したデータを用いてデータ破損を修復する。これにより、メモリデバイス３０の蓄積効率を高くすることができ、また、修復用の正常データをサーバ１０から取得する際のデータ通信時間を短くすることができる。



【特許請求の範囲】
【請求項１】
耐タンパ性のメモリ領域と非耐タンパ性のメモリ領域とを備え、前記非耐タンパ性のメモリ領域にデータを格納し、前記耐タンパ性のメモリ領域に前記データの破損の検査に用いる検査情報を格納したメモリデバイス。
【請求項２】
データを格納する非耐タンパ性の第１のメモリ領域と、データ破損の検査に用いる検査情報を格納する耐タンパ性の第２のメモリ領域と、外部から取得したデータを前記第１のメモリ領域に書き込み、前記検査情報を前記第２のメモリ領域に書き込む書き込み手段と、前記検査情報を用いてデータ破損を検査する検査手段と、前記検査手段が正常と判定したデータを読み出す読み出し手段とを備え、前記検査手段は、外部から取得した前記データをブロック単位で正常か否かを判定するメモリデバイス。
【請求項３】
前記検査情報が、外部から取得した前記データのブロック単位の検査情報を含み、前記書き込み手段は、前記検査情報を前記第２のメモリ領域に書き込む請求の範囲２記載のメモリデバイス。
【請求項４】
前記書き込み手段は、前記検査情報を暗号通信路を通じて取得し、前記検査情報を前記第２のメモリ領域に書き込む請求の範囲２記載のメモリデバイス。
【請求項５】
前記書き込み手段は、前記検査情報を暗号通信路を通じて取得し、前記検査情報を前記第２のメモリ領域に書き込む請求の範囲３記載のメモリデバイス。
【請求項６】
前記書き込み手段は、外部から取得した前記検査情報に付されている署名を検証した後、前記検査情報を前記第２のメモリ領域に書き込む請求の範囲３記載のメモリデバイス。
【請求項７】
前記書き込み手段は、データ破損の検査に用いる検査情報を取得して前記検査情報を検証する検証用検査情報を作成し、前記検証用検査情報を前記第２のメモリ領域に書き込み、データ破損の検査に用いる前記検査情報を前記第１のメモリ領域に書き込む請求の範囲２記載のメモリデバイス。
【請求項８】
前記書き込み手段は、署名付きの前記検査情報を取得して、前記署名付きの検査情報を検証する検証用検査情報を作成し、前記検証用検査情報を前記第２のメモリ領域に書き込み、前記署名付きの検査情報を前記第１のメモリ領域に書き込む請求の範囲７記載のメモリデバイス。
【請求項９】
前記書き込み手段は、前記検査情報を用いて前記第１のメモリ領域に書き込むデータの破損を検査し、正常なデータを前記第１のメモリ領域に書き込む請求の範囲２記載のメモリデバイス。
【請求項１０】
前記検査情報が、検査対象のデータの取得先を示す発行元情報を含み、前記検査手段は、前記検査情報を用いてデータ破損が生じているブロック単位を検出したとき、前記発行元情報と前記ブロック単位を示す情報とを含むエラー報告を出力する請求の範囲２記載のメモリデバイス。
【請求項１１】
前記検査情報が、検査対象のデータの取得先を示す発行元情報を含み、前記検査手段は、前記検査情報を用いてデータ破損が生じているブロック単位を検出したとき、前記発行元情報と前記ブロック単位を示す情報とを含むエラー報告を出力する請求の範囲３記載のメモリデバイス。
【請求項１２】

前記検査情報が、検査対象のデータの取得先を示す発行元情報を含み、前記検査手段は、前記検査情報を用いてデータ破損が生じているブロック単位を検出したとき、前記ブロック単位のデータの前記発行元に対する配信要求を出力する請求の範囲２記載のメモリデバイス。

【請求項１３】

前記検査情報が、検査対象のデータの取得先を示す発行元情報を含み、前記検査手段は、前記検査情報を用いてデータ破損が生じているブロック単位を検出したとき、前記ブロック単位のデータの前記発行元に対する配信要求を出力する請求の範囲３記載のメモリデバイス。

【請求項１４】

前記検査手段は、データ破損が生じているブロック単位の検査を自発的に行う請求の範囲１０記載のメモリデバイス。

【請求項１５】

前記検査手段は、データ破損が生じているブロック単位の検査を自発的に行う請求の範囲１１記載のメモリデバイス。

【請求項１６】

前記検査手段は、データ破損が生じているブロック単位の検査を自発的に行う請求の範囲１２記載のメモリデバイス。

【請求項１７】

前記検査手段は、データ破損が生じているブロック単位の検査を自発的に行う請求の範囲１３記載のメモリデバイス。

【請求項１８】

データ破損が生じているブロック単位を検出する前記検査手段の検出回数が閾値を越えたとき、動作を停止する請求の範囲２記載のメモリデバイス。

【請求項１９】

前記読み出し手段は、前記検査手段が正常と判定したブロック単位のデータを順次読み出す請求の範囲２記載のメモリデバイス。

【請求項２０】

外部から取得した前記ブロック単位のデータを前記検査情報を用いて検査し、前記データが正常であるとき、当該データを、前記第１のメモリ領域に書き込む修正手段を備える請求の範囲２記載のメモリデバイス。

【請求項２１】

前記エラー報告に対応したブロック単位のデータを外部から取得し、前記データを前記検査情報を用いて検査し、前記データが正常であるとき、当該データを、前記第１のメモリ領域に書き込む修正手段を備える請求の範囲１０記載のメモリデバイス。

【請求項２２】

前記エラー報告に対応したブロック単位のデータを外部から取得し、前記データを前記検査情報を用いて検査し、前記データが正常であるとき、当該データを、前記第１のメモリ領域に書き込む修正手段を備える請求の範囲１１記載のメモリデバイス。

【請求項２３】

暗号化データを復号化する復号化手段を備え、前記復号化手段は、前記検査手段が正常と判定した暗号化データのブロック単位のみを復号化し、前記読み出し手段は、前記復号化手段が復号化したブロック単位のデータを順次読み出す請求の範囲２記載のメモリデバイス。

【請求項２４】

暗号化データを復号化する復号化手段を備え、前記検査手段は、前記検査情報を用いて、前記復号化手段が復号化したブロック単位のデータに含まれるデータ破損を検査し、前記読み出し手段は、前記検査手段が正常と判定したブロック単位のデータを順次読み出す請求の範囲２記載のメモリデバイス。

【請求項２５】

検査対象のデータに先行して前記検査情報を更新する検査情報更新手段を備え、前記データの前記第１のメモリ領域への書き込みを前記修正手段が行う請求の範囲２０記載のメモリデバイス。

【請求項２６】

データをメモリデバイスの非耐タンパ性のメモリ領域に格納し、前記データの破損の検査に用いる検査情報を前記メモリデバイスの耐タンパ性のメモリ領域に格納する端末装置。

【請求項２７】

ブロック単位に分けたデータと、各ブロックのデータ破損を検査するための検査情報とをサーバから取得し、前記データをメモリデバイスにおける非耐タンパ性の第１のメモリ領域に格納し、前記検査情報を前記メモリデバイスにおける耐タンパ性の第２のメモリ領域に格納する端末装置。

【請求項２８】

前記メモリデバイスから、データ破損が生じているブロックを示すエラー報告を得て、当該ブロックのデータを前記サーバから取得し、前記メモリデバイスの第１のメモリ領域に格納する請求の範囲２７記載の端末装置。

【請求項２９】

前記メモリデバイスから、データ破損が生じているブロック単位のデータの発行元に対する配信要求が出力されたとき、当該ブロックのデータを前記発行元のサーバから取得し、前記メモリデバイスの第１のメモリ領域に格納する請求の範囲２７記載の端末装置。

【請求項３０】

前記メモリデバイスからの前記エラー報告の回数または前記配信要求の回数が閾値を越えたとき、前記サーバからのデータ取得を停止する請求の範囲２８記載の端末装置。

【請求項３１】

前記メモリデバイスからの前記エラー報告の回数または前記配信要求の回数が閾値を越えたとき、前記サーバからのデータ取得を停止する請求の範囲２９記載の端末装置。

【請求項３２】

データと前記データの破損を検査する検査情報とを管理するサーバと、前記サーバから前記データ及び検査情報を取得する端末装置と、前記端末装置が前記サーバから取得した前記データを非耐タンパ性のメモリ領域に格納し、前記検査情報を耐タンパ性のメモリ領域に格納するメモリデバイスとを備え、前記メモリデバイスは、前記検査情報を用いて前記データの破損を検出し、前記端末装置は、破損が検出されたデータを前記サーバから取得し、前記メモリデバイスは、前記端末装置が取得したデータを用いてデータの破損を修復するデータ修復システム。

【請求項３３】

ブロック単位に分けたデータと各ブロックのデータ破損を検査するための検査情報とを管理するサーバと、前記サーバから前記データと前記検査情報とを取得する端末装置と、前記端末装置が取得した前記データを非耐タンパ性の第１のメモリ領域に格納し、前記検査情報を耐タンパ性の第２のメモリ領域に格納するメモリデバイスとを備え、前記メモリデバイスは、前記検査情報を用いてデータ破損が生じているブロックを検出し、前記端末装置は、検出された前記ブロックのデータを前記サーバから取得し、前記メモリデバイスは、前記端末装置が取得したデータを用いてデータ破損を修復するデータ修復システム。

【請求項３４】

前記端末装置は、前記サーバから前記検査情報を前記データに先行して取得し、前記メモリデバイスは、前記検査情報を格納し、前記データの読み出し要求があったときに、未蓄積の前記データをデータ破損が生じているデータとして検出し、これを受けた前記端末装置が、前記データを前記サーバから取得して、前記メモリデバイスに格納する請求の範囲３３記載のデータ修復システム。

【請求項３５】

データを格納する非耐タンパ性の第１のメモリ領域と、データ破損の検査に用いる検査情報を格納する耐タンパ性の第２のメモリ領域と、外部から取得したデータを前記第１のメ

モリ領域に書き込み、前記検査情報を前記第２のメモリ領域に書き込む書き込み手段と、前記外部から取得したデータの破損を前記検査情報を用いて検査する検査手段と、前記検査手段が正常と判定したデータを読み出す読み出し手段とを備えるメモリデバイス。

【請求項３６】

データとこのデータの破損を検査するための検査情報とをサーバから取得し、前記データをメモリデバイスにおける非耐タンパ性の第１のメモリ領域に格納し、前記検査情報を前記メモリデバイスにおける耐タンパ性の第２のメモリ領域に格納する端末装置。

【請求項３７】

データとこのデータの破損を検査するための検査情報とを管理するサーバと、前記サーバから前記データと前記検査情報とを取得する端末装置と、前記端末装置が取得した前記データを非耐タンパ性の第１のメモリ領域に格納し、前記検査情報を耐タンパ性の第２のメモリ領域に格納するメモリデバイスとを備え、前記メモリデバイスは、前記検査情報を用いて前記データの破損の有無を検出し、前記端末装置は、前記破損が検出されたデータを前記サーバから取得し、前記メモリデバイスは、前記端末装置が取得したデータを用いてデータ破損を修復するデータ修復システム。

【発明の詳細な説明】

技術分野

本発明は、ダウンロードしたデータの破損箇所を修復する修復システムと、そのシステムを構成するメモリデバイス及び端末装置に関し、特に、メモリデバイスに記録されたデータを効率的に修復できるようにするものである。

背景技術

従来から、端末装置の処理を規定するプログラムなどのデータを、サーバからネットワークを通じて端末装置にダウンロードすることは広く行われている。端末装置の記憶手段に格納されたデータは、ダウンロード時の送信異常や、ハード装置の故障、ウィルスによるデータ消失、外部からの攻撃による破壊など、様々な原因で破損する場合がある。

こうしたデータの破損は、サーバがデータとともに伝送したチェックサムなどの検査情報と、記憶手段に格納したデータから計算したチェックサムとの一致を検査することにより発見できる。

蓄積したデータを外部からの破壊や改竄から守る必要がある場合は、ＩＣカードなどの耐タンパ性（外部からの攻撃に対する耐性）を備えた記憶手段にデータを格納することが行われている。耐タンパ性は、ダミー回路を設けたり、処理時間を一定時間内に制限したり、熱や電磁波の影響を受けない構造にしたりして実現される。

また、破損してしまったデータを修復する方法として、特開平４－３４０１５０号公報には、データの異常を発見した場合に、端末装置がサーバにダウンロード要求を発し、サーバから改めてプログラムデータのダウンロードを受ける方式が記載されている。

また、特開平１１－１８４７０５号公報には、端末装置が第１及び第２の記憶手段を持ち、ダウンロードされたデータをこれらの記憶手段の双方に重複して格納し、第１の記憶手段で記憶するデータが破損した場合に、第２の記憶手段で記憶するデータを第１の記憶手段に上書きする方式が記載されている。

しかし、耐タンパ性の記憶装置は、コストが高く、また、多くの記憶容量を確保することができない。そのため、データ量の多い音楽データなどを蓄積することは不可能である。

また、データの破損が発見された際にサーバから改めてデータのダウンロードを受ける方式では、そのダウンロードのために多くの通信時間が必要になると言う問題点がある。

また、データを重複して保持する方式では、端末装置が多くの記憶容量を備えた記憶手段を持たなければならないと言う問題点がある。

また、近年は携帯端末による、物品やエンタテイメントコンテンツデータの購入、ネットバンキングなどのＥＣ（電子商取引）が浸透し始めている。また、アドレス帳やスケジュール管理の用途としても用いられている。これらの情報をネットワーク上のサーバで管理することも可能であるが、情報を取り出すまでにかかるタイムラグや、ネットワーク障害時に必要な情報にアクセスできない場合があるという問題をかかえることになる。よって

、これらの情報を含めて、携帯端末で取り扱うデータの記憶媒体として、すぐにアクセス可能で、十分な容量を持つカードデバイスの需要は大きい。しかし、同時に、カードデバイスの情報が破損した際に、確実にかつ少ないコスト（時間含む）で情報を修復できないと、それらの情報の処理にとって障害となるばかりではなく、ユーザに対して不利益を与え、新しいサービスの普及にとって大きな妨げとなってしまう。また、新しいサービスが拡大して行かないことは、ＩＴ（Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｅｃｈｎｏｌｏｇｙ）技術そのものの発展にとっても妨げとなる。

発明の開示

本発明の目的は、破損したデータの修復を効率的に行うことができるデータ修復システムと、そのシステムを実現するメモリデバイス及び端末装置を提供することである。

この目的は、耐タンパ性のメモリ領域と非耐タンパ性のメモリ領域とをメモリデバイスに設け、非耐タンパ性のメモリ領域にデータを格納し、耐タンパ性のメモリ領域に前記データの破損の検査に用いる検査情報を格納することにより達成される。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を用いて説明する。なお、本明細書においてデータの破損とは、データが本来のデータから変化したり、データが欠落したりしたものを言う。

（実施の形態１）

本発明の実施形態１におけるデータ修復システムは、図１に示すように、ダウンロードの対象のデータを管理するサーバ１０と、サーバ１０との伝送路を確保してダウンロードされるデータを受信する端末２０と、端末２０に装着されてダウンロードしたデータを記憶するメモリデバイス３０とで構成される。

ダウンロード対象のデータは、ユーザによるデータの変更を許さないプログラムデータや音楽データ、地図データなどの不変データである。サーバ１０は、これらのデータを複数のブロックに分割して、各ブロックに、そのブロックのデータに対する検査情報（ハッシュ値、チェックサム、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）、署名など）を生成し、そのデータ本体と検査情報とを保持・管理する。そして、端末２０からデータの要求があると、そのデータのデータ本体と検査情報とを端末２０にダウンロードする。

図３は、検査情報の一例を示している。この検査情報には、データのファイル名と、データ取得先のサーバ名やＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）、データ発行会社名などを表す発行元の情報と、ファイルサイズと、各ブロックのブロックサイズと、各ブロックのハッシュ値とが含まれている。

メモリデバイス３０は、メモリカード等と称せられる記憶媒体であり、フラッシュメモリ等から成るメモリ３１と、メモリ３１へのデータの書き込み／読み出しを制御するメモリコントローラ３２とを備えている。メモリコントローラ３２は、耐タンパ性を備えているが、メモリ３１は非耐タンパである。サーバ１０からダウンロードされたデータの内、データ本体はメモリデバイス３０のメモリ３１の領域に格納され、検査情報はメモリコントローラ３２に格納される。

図２は、メモリデバイス３０のハード構成を示している。メモリコントローラ３２は、メモリデバイス３０の動作を制御するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）３２３と、ＣＰＵ３２３が作業領域として使用するＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）３２２と、ＣＰＵ３２３の動作を規定するプログラムが格納されたＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）３２１と、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）等から成る耐タンパ性を有する内部不揮発性メモリ３２４と、端末２０との間でデータを入出力する入出力部（Ｉ／Ｏ）３２５と、メモリ３１との間のＩ／Ｏ３２６とを備えている。

図５は、メモリデバイス３０におけるデータ処理を模式的に示している。メモリコントローラ３２は、メモリ３１にデータ本体を書き込み、内部不揮発性メモリ３２４に検査情報

を書き込む書込部３２７と、検査情報を用いてデータ本体の破損を検出する検査部３２８と、メモリ３１に格納されたデータ本体を外部に読み出す読出部３２９とを備えている。この書込部３２７、検査部３２８及び読出部３２９の各機能は、ＣＰＵ３２３がプログラムで規定された処理を行うことにより実現される。

サーバ１０からダウンロードしたデータをメモリデバイス３０に書き込む場合、端末２０は、サーバ１０から取得したデータ本体と検査情報とを書き込み要求とともにメモリデバイス３０に出力する。

書込部３２７は、図６のフロー図に示すように、

ステップＳＴ１：各ブロックのハッシュ情報を含む検査情報を内部不揮発性メモリ３２４に書き込む。

ステップＳＴ２：ファイルのデータ本体をメモリ３１に書き込む。

この書き込み処理が終了すると、書込部３２７は、端末２０に書き込み完了通知を出力する。

また、メモリデバイス３０からデータを読み出す場合は、読み出すべきデータの破損の有無が検査される。この場合、端末２０からメモリデバイス３０に、選択したファイルのデータ破損の検査要求が入力し、検査部３２８は、図８のフロー図に示す処理を行う。

ステップＳＴ１０：内部不揮発性メモリ３２４から検査情報を読み出し、その中の“ブロックサイズ”の情報を基に各ブロックの範囲を確認し、メモリ３１に格納されたデータ本体の着目するブロックのデータに対するハッシュ値を計算する。

ステップＳＴ１１：算出したハッシュ値と、検査情報に含まれる該当するブロックのハッシュ値とを比較し、それらが一致しないときは、ステップＳＴ１３に進む。

ステップＳＴ１３：そのブロック位置を特定する情報とブロックサイズと発行元の情報とを含むエラー報告を作成し、このエラー報告を検査結果として端末２０に出力する。

また、ステップＳＴ１１において、算出したハッシュ値と検査情報に含まれる該当するブロックのハッシュ値とが一致するときは、ステップＳＴ１２に進む。

ステップＳＴ１２：最終ブロックに達するまで、順次ブロックを変えてステップＳＴ１０以下の処理を繰り返し、最終ブロックに達した場合は検査処理を終了して、“正常”を表す検査結果を端末２０に出力する。

エラーの検査結果を受けた端末２０は、破損データを含むブロックのデータをサーバ１０から取得し、メモリデバイス３０は、これを用いてメモリ３１のデータを修復する。図９は、このデータ修復処理の手順を模式的に示している。このメモリデバイス３０のメモリコントローラ３２は、内部不揮発性メモリ３２４及び検査部３２８の他に、メモリ３１に格納されたデータを修復する修正部３３０を備えている。この修正部３３０の機能は、ＣＰＵ３２３がプログラムで規定された処理を行うことにより実現される。

端末２０から破損データの検査要求が入力すると（１）、メモリデバイス３０の検査部３２８は、図８の手順により、データ破損が生じているブロック位置を特定する情報、ブロックサイズ及び発行元情報を含むエラー報告を検査結果として端末２０に出力する（２）。

端末２０は、このエラー報告をトリガーとして、データ破損が生じているブロックのデータを発行元のサーバ１０に要求する。サーバ１０は、管理するデータの中から、該当するブロックのデータ本体を読み出して端末２０にダウンロードする（３）。

図１０は、この模様を模式的に示している。端末２０は、メモリデバイス３０から受信した発行元（ＵＲＬ）、破損データを含むブロック位置、ブロックサイズを基に、サーバ１０に対して、破損データを含むブロックの正常データ（部分データ）を要求する（▲１▼）。サーバ１０は、検査情報を参照し、要求された部分データを端末２０に返送する（▲２▼）。このように、サーバ上のファイルの特定位置から特定サイズ分の情報を取得することは既知の技術であり、既存のＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）や、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）サーバにおいても行われている。

修正すべきブロックのデータ本体を取得した端末２０は、このデータ本体と修正すべきブ

ロックを指定する情報とを含む部分修正情報を作成して、修正要求とともにメモリデバイス３０に出力する（４）。
部分修正情報を受信したメモリデバイス３０の修正部３３０は、図１１に示す手順でデータの修復を実行する。
ステップＳＴ２０：部分修正情報に含まれるブロックのデータ本体のハッシュ値を計算する。
ステップＳＴ２１：算出したハッシュ値と、内部不揮発性メモリ３２４に格納された検査情報に含まれる該当するブロックのハッシュ値とを比較する。それらが一致しないときは、ステップＳＴ２４に進む。
ステップＳＴ２４：端末２０にそのブロックのデータ本体を再取得するように促す“再書き込み用前処理”を行い、データ本体が再取得された場合に、ステップＳＴ２０からの手順を繰り返す。
また、ステップＳＴ２１において、算出したハッシュ値と検査情報に含まれる該当するブロックのハッシュ値とが一致するときは、ステップＳＴ２２に進む。
ステップＳＴ２２：そのデータ本体をメモリ３１に上書きする。
ステップＳＴ２３：部分修正情報の中に他のブロックのデータ本体が含まれている場合は、ステップＳＴ２０以降の手順を繰り返し、部分修正情報の中に書きむべきデータ本体が無くなれば修復処理を終了する。
こうしてデータの修復処理が終了すると、修正部３３０は、端末２０に修正完了通知を出力する（５）。
データが修復された場合、検査部３２８の検査結果は“正常”になる。
端末２０がメモリデバイス３０から“正常”の検査結果を得たファイルデータの読み出しを要求すると、メモリデバイス３０の読出部３２９は、メモリ３１から該当するデータ本体を読み出して端末２０に出力する。
また、端末２０がメモリデバイス３０に、データ破損の検査を経ずに、ファイルデータの読み出しを要求した場合には、読出部３２９から検査部３２８に対して、読み出そうとする各ブロックのデータ破損についての検査要求が出され、“正常”の検査結果が得られたブロックのデータが順次読み出される。図１２のフロー図は、この読み出し処理の動作を示している。
ステップＳＴ３０：ファイルデータの読み出し要求を受けた読出部３２９は、要求されたファイル名を検査部３２８に伝えて、ファイルデータの破損の検査を要求する。
読出部３２９から検査要求を受けた検査部３２８は、内部不揮発性メモリ３２４から該当するファイルの検査情報を読み出し、ブロックサイズから各ブロックの範囲を確認して、メモリ３１に格納されたデータ本体の着目するブロックのデータに対するハッシュ値を計算する。
ステップＳＴ３１：算出したハッシュ値と、検査情報に含まれる該当するブロックのハッシュ値とを比較する。それらが一致しないときは、ステップＳＴ３４に進む。
ステップＳＴ３４：そのブロック位置を特定する情報とブロックサイズと発行元の情報とを含むエラー報告を作成し、このエラー報告を検査結果として読出部３２９に出力する。
エラー報告を受けた読出部３２９は、エラー報告を端末２０に出力する。
また、ステップＳＴ３１において、計算したハッシュ値と検査情報に含まれる該当するブロックのハッシュ値とが一致するときは、ステップＳＴ３２に進む。
ステップＳＴ３２：検査部３２８は、ブロック位置を特定する情報と、そのブロックが“正常”であることを表す情報とを検査結果に含めて読出部３２９に伝え、読出部３２９は、そのブロックのデータ本体をメモリ３１から読み出す。
ステップＳＴ３３：指定されたファイルの最終ブロックに達するまで、順次ブロックを変えてステップＳＴ３０以下の処理を繰り返し、最終ブロックに達した場合は読み出し処理を終了する。
また、読出部３２９からエラー報告を受けた端末２０は、このエラー報告をトリガーとして、データ破損が生じているブロックのデータ本体を発行元のサーバ１０から取得し、メ

モリデバイス３０は、それを用いてデータの修復処理を行う。この処理は、図９及び図１１で示したものと同じである。そして、修復されたデータの検査結果は“正常”となり、読出部３２９は、修復されたデータ本体をメモリ３１から読み出す。
この読み出し処理では、検査結果が“正常”と判定されたブロックのデータ本体を直ぐに読み出しているため、検査終了からデータ読み出しの間にデータ破損が発生する可能性をゼロにすることができる。
このように、このデータ修復システムでは、メモリデバイスに蓄積したデータが破損しているとき、正常データを外部から取得して修復しているため、バックアップ用のデータを重複して保持する場合に比べて、メモリデバイスの蓄積効率を高めることができる。また、検査情報の生成単位を、データ全体ではなく、ブロック単位としているため、データ破損個所を小さな範囲に限定することができ、修復用の正常データを外部から取得する際のデータ通信時間を短縮することができる。
また、この検査情報をメモリデバイスの耐タンパ性の蓄積領域に格納し、データ本体をメモリデバイスの非タンパ性の蓄積領域に格納しているため、ＩＣカードのように全ての情報を耐タンパ性の蓄積領域に格納する場合に比べて、メモリデバイスの構成を簡素化することができ、低コストでの製造が可能になる。また、耐タンパ性の蓄積領域に格納した検査情報は、データ破壊や改竄から守ることができるため、データ本体が破損した場合でも、この検査情報を用いてデータ破損を確実に検出することができ、正常データを外部から取得して完全に修復することができる。
なお、図３では、ファイル名を含む検査情報の例を示したが、図４に示すように、検査情報にファイル名を含めないことも可能である。この場合、発行元の情報としてファイル取得先のＵＲＬを表すようにすれば、ファイルごとにＵＲＬが異なり、ＵＲＬでファイルが特定できるので、検査情報へのファイル名の記述が不要になる。
また、検査情報で各ブロックのデータ本体を格納するメモリデバイスのメモリ領域を指定し、図４に示すように、そのメモリ領域を表すブロック番号と、そのメモリ領域に格納するデータ本体のハッシュ値とを対応付けて検査情報に記述するようにすれば、メモリデバイス３０の検査部３２８がメモリ３１に格納されたデータ本体の破損をチェックする場合に、その処理が容易になる。
また、図６では、サーバ１０からダウンロードしたデータをメモリデバイス３０に取り敢えず書き込み、読み出し時にデータ破損を検出する場合の書き込み手順について示しているが、データの書き込み時にデータ破損をチェックし、正常なデータを書き込むようにすることも可能である。この場合、図５の書込部３２７及び検査部３２８により、図７のフロー図に示す書き込み処理が行われる。
ステップＳＴ４０：メモリデバイス３０の書込部３２７は、各ブロックのハッシュ情報を含む検査情報を内部不揮発性メモリ３２４に書き込み、ステップＳＴ４１に進む。
ステップＳＴ４１：一つのブロックのデータ本体をメモリ３１に書き込む。
ステップＳＴ４２：検査部３２８は、このブロックのデータ本体のハッシュ値を計算し、ステップＳＴ４３に進む。
ステップＳＴ４３：算出したハッシュ値と、内部不揮発性メモリ３２４に格納した検査情報に含まれる該当するブロックのハッシュ値とを比較する。それらが一致しないときは、ステップＳＴ４５に進む。
ステップＳＴ４５：端末２０にそのブロックのデータ本体を再取得するように促し、また、再取得したデータ本体の書き込み位置を元のデータ本体が書き込まれていたメモリ３１上の位置から変更する“再書き込み用前処理”を行い、データ本体が再取得された場合に、ステップＳＴ４１からの手順を繰り返す。なお、データ本体の書き込み位置の変更は、データ破損の生じたメモリ領域が、物理的に壊れている可能性があり、そのための措置である。
また、ステップＳＴ４３において、算出したハッシュ値と検査情報に含まれる該当するブロックのハッシュ値とが一致するときは、ステップＳＴ４４に進む。
ステップＳＴ４４：そのブロックが最終ブロックであるか否かを識別し、最終ブロックで

なければ、ステップＳＴ４１以降の手順を繰り返し、最終ブロックであれば、書き込み処理を終了する。
書き込み処理が終了すると、書込部３２７は、端末２０に書き込み完了通知を出力する。
こうした処理により、データ破損を含まないデータ本体の書き込みが保証され、データ読み出し時の検査において、データ破損が発生する割合を低減することができる。
また、ここでは、端末が、メモリデバイスからエラー報告を受けて、データ破損を含むブロックデータの再取得を実行しているが、これは、メモリデバイスが、端末に対して、データの発行元とブロック位置とを指定して発行元への配信要求命令を出し、端末がその命令に従って発行元からデータを再取得する、と言う形態であっても良い。
また、このデータ修復システムでは、検査情報の生成単位をブロック単位とし、データ破損個所を小さな範囲に限定しているため、データが破損したブロックの情報を収集、解析して有益な情報を得ることができる。
サーバは、各端末からデータ復旧のために要求されたブロックの統計情報から次のような解析が可能である。
固定データの同一個所の破損が多数のユーザで発生する場合は、▲１▼プログラムのバグによるデータ破壊の可能性がある。▲２▼データ（例えば、音楽ファイルなど）の不正利用方法が流布している可能性がある。
また、プログラムの同一個所の破損が多数のユーザで発生する場合は、▲１▼ウィルスによるプログラム改竄の可能性がある。▲２▼プログラム不正改造方法が流布している可能性がある。
また、同一ユーザによる修正が頻発する場合は、メモリデバイスのハードウェアが故障している可能性があり、この解析結果を基に、メモリデバイスの修理や交換を勧める情報を端末に送るなどのサービスが可能になる。
また、端末は、メモリデバイスからのエラー報告の回数が閾値を越えた場合、あるいは、一定時間内に閾値を越えるエラー報告を受けた場合に、メモリデバイスのハードウェア故障や外部からの攻撃の可能性があるものと見て、▲１▼メモリデバイスからのエラー報告の受付を停止する、▲２▼エラー報告のサーバへの送出を停止する、▲３▼サーバからの修復データの取得を停止する、▲４▼メモリデバイスを交換する、等の措置を取ることができる。
また、端末は、メモリデバイスの利用回数が閾値を越えた場合、メモリデバイスの寿命が尽きる前に、新しいメモリデバイスにデータを移し変える措置を取ることもできる。
また、データ破損の頻度により、メモリデバイス自身がデータ修復の自律機能を停止するようにしても良い。自律機能の停止とは、書込部３２７、検査部３２８、読出部３２９などの、データ取得や読み出しに必要なメモリデバイス内の全部または一部の諸機能を停止させることである。自律機能停止の条件は、データ破損の検出回数が閾値を越えた場合、あるいは、一定期間内に閾値を越えるデータ破損を検出した場合などであり、停止の形態は、▲１▼一定期間（一定周期）停止する、▲２▼次回のリセットまで停止する、▲３▼完全停止する（この場合、専門業者に依頼して機能回復を図る）、などである。
（実施の形態２）
実施の形態２では、暗号化されたデータ本体をメモリデバイスに格納するデータ修復システムについて説明する。
このメモリデバイスは、図１３に示すように、メモリコントローラ３２が、暗号化データを復号化する暗号コプロセッサ３３１を備えている。その他の構成は実施の形態１（図２）と変わりがない。
図１４は、このメモリデバイス３０におけるデータ処理を模式的に示している。メモリコントローラ３２は、書込部３２７、検査部３２８、読出部３２９及び内部不揮発性メモリ３２４の他に、暗号化データを復号化する復号部３３２を備えている。この復号部３３２の機能は、暗号コプロセッサ３３１により実現される。
このシステムのサーバ１０は、ファイルデータを暗号化した後、複数のブロックに分割し、各ブロックのデータに対する検査情報（ハッシュ値、チェックサム、ＣＲＣ、署名など

）を生成して、その暗号化データと検査情報とを保持・管理する。そして、端末２０からデータの要求があると、暗号化データと検査情報とを端末２０にダウンロードする。
端末２０は、サーバ１０から取得した暗号化データと検査情報とを書き込み要求とともにメモリデバイス３０に出力する。
メモリコントローラ３２の書込部３２７は、図６または図７に示す手順で、検査情報を内部不揮発性メモリ３２４に、また、暗号化データをメモリ３１に書き込む。
メモリコントローラ３２の検査部３２８は、暗号化データの破損を検査する場合、メモリ３１に格納された各ブロックの暗号化データのハッシュ値を計算し、算出したハッシュ値と、内部不揮発性メモリ３２４に格納された検査情報に含まれる該当するブロックのハッシュ値とを比較する。そして、それらが一致するときは“正常”の検査結果を出力し、不一致であるときはエラー報告を出力する。
また、メモリデバイス３０に格納されたデータを読み出す場合は、検査部３２８の検査結果が“正常”であるブロックの暗号化データが復号部３３２で復号化され、読出部３２９から読み出される。
その他の動作は実施の形態１と変わりがない。
また、図１５は、データを暗号化する場合の他の形態を示している。
このシステムのサーバ１０は、ファイルデータを複数のブロックに分割し、各ブロックのデータに対する検査情報を生成した後、各ブロックのデータを暗号化し、その暗号化データと検査情報とを保持・管理する。そして、端末２０からデータの要求があると、暗号化データと検査情報とを端末２０にダウンロードする。
端末２０は、サーバ１０から取得した暗号化データと検査情報とを書き込み要求とともにメモリデバイス３０に出力する。
メモリコントローラ３２の書込部３２７は、図１４の場合と同様に、検査情報を内部不揮発性メモリ３２４に、また、暗号化データをメモリ３１に書き込む。
メモリコントローラ３２の検査部３２８は、暗号化データの破損を検査する場合、メモリ３１に格納された各ブロックの暗号化データを復号部３３２で復号化し、得られたデータのハッシュ値を計算して、検査情報に含まれる該当するブロックのハッシュ値と比較する。そして、それらが一致するときは“正常”の検査結果を出力し、不一致であるときはエラー報告を出力する。
また、読出部３２９は、検査部３２８の検査結果が“正常”である場合にだけ、復号部３３２で復号化されたデータを外部に読み出す。
その他の動作は実施の形態１と変わりがない。
このように、図１４では、暗号化したデータの検査情報を用いてデータ破損を検査し、図１５では、復号化したデータの検査情報を用いてデータ破損を検査しているが、いずれの場合でも、暗号化データを復号化して読み出すには、必ず検査部の検査手順を通らなければならない。
このシステムでは、サーバと端末との間で、データが暗号化されて伝送され、また、メモリデバイスの非耐タンパのメモリ領域にデータが暗号化されて蓄積されるため、データのセキュリティを守ることができる。
なお、ここでは、メモリコントローラ３２に暗号コプロセッサ３３１を設ける場合について説明したが、暗号コプロセッサ３３１の機能をＣＰＵ３２３が代わって行うようにしても良い。
（実施の形態３）
実施の形態３では、検査情報の改竄防止の措置を講じたデータ修復システムについて説明する。
このシステムでは、サーバが端末に対して、ブロックに分割したデータと、署名を付した検査情報とをダウンロードし、メモリデバイスは、検査情報を格納する際に、その署名を検証する。
図１６は、このメモリデバイス３０のデータ処理を模式的に示している。メモリコントローラ３２は、書込部３２７及び内部不揮発性メモリ３２４の他に、検査情報の署名を検証

する署名検証部３３３を備えている。この署名検証部３３３の機能は、ＣＰＵ３２３がプログラムで規定された処理を行うことにより実現される。
このシステムのサーバ１０は、複数のブロックに分割したデータと、その検査情報とを保持・管理し、端末２０からデータの要求があったときに、データ本体と、署名を付した検査情報とを端末２０にダウンロードする。
端末２０は、サーバ１０から取得したデータと署名付きの検査情報とを書き込み要求とともにメモリデバイス３０に出力する。
メモリコントローラ３２の書込部３２７は、署名付きの検査情報を署名検証部３３３に渡し、データ本体をメモリ３１に書き込む。
署名検証部３３３は、検査情報に付された署名を検証し、検査情報が改竄されていないことを確認した後、検査情報を内部不揮発性メモリ３２４に格納する。
その他の処理は実施の形態１と変わりがない。
このシステムでは、検査情報に付された署名を検証することで、サーバから送信された検査情報が、メモリデバイスの耐タンパ性のメモリ領域に格納される以前に悪意の第３者によって改竄される事態を防止することができる。
また、図１７は、検査情報の改竄を防止するため、検査情報を暗号通信路で伝送する場合を示している。
このメモリコントローラ３２は、データをメモリ３１に書き込むデータ書込部３３６と、検査情報を内部不揮発性メモリ３２４に書き込む検査情報書込部３３５とを備えている。
このデータ書込部３３６及び検査情報書込部３３５の機能は、ＣＰＵ３２３がプログラムで規定された処理を行うことにより実現される。
このシステムでは、検査情報が、サーバ１０からメモリデバイス３０の検査情報書込部３３５に暗号通信路を通じて伝送される。この暗号通信路は、ＩＣカードにおけるセキュアメッセージングなどと同様に、サーバ１０と検査情報書込部３３５とが直接構築する。検査情報書込部３３５は、受信した検査情報を耐タンパ性の内部不揮発性メモリ３２４に書き込む。
また、データは、サーバ１０からメモリデバイス３０に通常の伝送路で伝送され、データ書込部３３６は、受信したデータをメモリ３１に書き込む。
このシステムでは、検査情報を暗号通信路で伝送しているため、検査情報が、メモリデバイスの耐タンパ性のメモリ領域に格納される以前に悪意の第３者によって改竄される事態を防ぐことができる。
（実施の形態４）
実施の形態４では、耐タンパ性のメモリ領域の使用効率を高めたデータ修復システムについて説明する。
メモリデバイスに格納するデータそのものが大きくなると、それに対応して検査情報のデータ量も増大し、検査情報を耐タンパ性のメモリ領域に書き込むことが困難になる。そのため、このシステムでは、検査情報をメモリデバイスの非耐タンパのメモリ領域に書き込み、その検査情報のデータ破損を検査するための検査情報（検査情報用検査情報）をメモリデバイスの耐タンパ性のメモリ領域に書き込むようにしている。
図１８は、このメモリデバイス３０のデータ処理を模式的に示している。メモリコントローラ３２は、図１６の場合と同様に、書込部３２７、署名検証部３３３及び内部不揮発性メモリ３２４を備えており、また、サーバ１０からは、データ本体と署名を付した検査情報とがダウンロードされる。
このメモリコントローラ３２の書込部３２７は、署名付きの検査情報を署名検証部３３３に渡し、署名検証部３３３が検査情報に付された署名を検証して、検査情報が改竄されていないことを確認すると、書込部３２７は、署名付きの検査情報とデータ本体とをメモリ３１に書き込む。
一方、署名検証部３３３は、検査情報及び署名に対するハッシュ値（即ち、検査情報用検査情報）を算出し、この検査情報用検査情報を内部不揮発性メモリ３２４に格納する。
この場合、検査部３２８は、ブロックのデータ破損を検査するとき、署名付き検査情報を

メモリ３１から読み出し、その検査情報に破損が生じていないことを、内部不揮発性メモリ３２４に格納された検査情報用検査情報を用いて確認する。その後の検査処理は実施の形態１と同じである。また、検査情報が破損しているときは、サーバから検査情報を取得し直す。

また、図１９は、メモリデバイス３０がサーバからデータ本体と署名無しの検査情報とを受信する場合のデータ処理を模式的に示している。このメモリコントローラ３２は、書込部３２７及び内部不揮発性メモリ３２４の他に検査情報用検査情報を生成する検査情報用検査情報生成部３３７を備えている。この検査情報用検査情報生成部３３７の機能は、ＣＰＵ３２３がプログラムで規定された処理を行うことにより実現される。

このシステムのサーバ１０は、データ本体と署名なしの検査情報とを端末２０にダウンロードする。なお、この検査情報は、図１７に示すように、暗号通信路を用いて伝送するようにしても良い。

このメモリコントローラ３２の書込部３２７は、データ本体と検査情報とを受信すると、検査情報を検査情報用検査情報生成部３３７に伝えるとともに、この検査情報とデータ本体とをメモリ３１に書き込む。

検査情報用検査情報生成部３３７は、検査情報のデータに対するハッシュ値（即ち、検査情報用検査情報）を算出し、この検査情報用検査情報を内部不揮発性メモリ３２４に格納する。

この場合、検査部３２８は、メモリ３１に格納されたデータ本体のデータ破損を検査するとき、検査情報をメモリ３１から読み出し、その検査情報に破損が生じていないことを、内部不揮発性メモリ３２４に格納された検査情報用検査情報を用いて確認する。その後の検査処理は実施の形態１と同じである。また、検査情報が破損しているときは、サーバから検査情報を取得し直す。

このシステムでは、検査情報そのものを非耐タンパのメモリ３１に置くことで、耐タンパ性のメモリ領域の使用量を削減することができる。この場合、非耐タンパのメモリ３１に格納した検査情報は、書き込んでから読み出すまでの間にデータ破損の生じる可能性があるが、耐タンパ性のメモリ領域で検査情報用検査情報を保持することにより、検査情報が正常であるか否かを判定することができ、検査情報が正常でないときには、サーバから検査情報を取り直すことにより、常に誤りのない検査情報を用いてデータ本体の破損を検査することができる。

（実施の形態５）

実施の形態５では、データ修復の機能を利用するシステムであって、検査情報のみを先にダウンロードし、データ本体は、それを使用する時にダウンロードするシステムについて説明する。

図２０は、このシステムでのメモリデバイス３０のデータ処理を模式的に示している。メモリコントローラ３２は、検査部３２８、読出部３２９、修正部３３０及び内部不揮発性メモリ３２４の他に、検査情報の更新処理を行う検査情報更新部３３４を備えている。この検査情報更新部３３４の機能は、ＣＰＵ３２３がプログラムで規定された処理を行うことにより実現される。

このシステムのサーバ１０は、例えば、新規作成したプログラムデータを複数のブロックに分割し、各ブロックのデータ本体と、その検査情報とを保持・管理する。そして、端末２０からの要求に応じて、あるいは、プッシュ型のサービスにより、その新規な検査情報のみを端末２０にダウンロードする。

端末２０は、サーバ１０から取得した新検査情報を、検査情報の更新要求とともにメモリデバイス３０に出力する。

メモリコントローラ３２の検査情報更新部３３４は、新検査情報を内部不揮発性メモリ３２４に書き込む。この新検査情報に対応するプログラムデータは、未だメモリ３１に格納されていない。

この新たなプログラムデータをユーザが使用するとき、ユーザの操作に基づいて端末２０からメモリデバイス３０にデータの読み出し要求が出力される（１）。

読み出し要求を受けたメモリコントローラ３２の読出部３２９は、図１２に示す手順で、検査部３２０に検査要求を出力する。検査部３２８は、内部不揮発性メモリ３２４から新検査情報を読み出し、また、メモリ３１に格納されたデータ本体を読み出して、そのデータのハッシュ値を計算しようとする。しかし、メモリ３１には該当するデータが格納されていないため、検査結果としてエラー報告を読出部３２９に出力する。エラー報告を受けた読出部３２９は、それを端末２０に出力する（２）。

端末２０は、このエラー報告をトリガーとして、検査情報に対応するプログラムデータを発行元のサーバ１０に要求し、サーバ１０は、そのプログラムデータを端末２０にダウンロードする。このデータを取得した端末２０は、このデータを含む部分修正情報を作成し、修正要求とともにメモリデバイス３０に出力する（３）。

部分修正情報を受信したメモリデバイス３０の修正部３３０は、図１１に示す手順でプログラムデータをメモリ３１に書き込み、端末２０に修正完了通知を出力する（４）。

プログラムデータがメモリ３１に書き込まれたことによって、検査部３２８は、そのデータが“正常”である旨の検査結果を読出部３２９に伝え、読出部３２９は、そのプログラムデータをメモリ３１から読み出して端末２０に出力する（５）。

このように、このシステムでは、メモリデバイス内で保持する検査情報を先行して更新し、その検査情報に対応するデータ本体の更新を、その使用時まで遅らせることができる。

図２１は、このシステムの応用例として、サーバ１０が、検査情報とカタログ情報とを先行して端末２０にダウンロードし、ユーザがカタログ情報で表示するコンテンツを希望したとき、そのコンテンツのデータを端末２０にダウンロードするシステムの手順を示している。まず、▲１▼端末２０は、サーバ１０からカタログ情報と検査情報とを取得する。

▲２▼端末２０は、メモリデバイス３０に、取得したカタログ情報と検査情報とを書き込む。カタログ情報及び検査情報は、メモリデバイス３０の耐タンパ性のメモリ領域に書き込まれる。

▲３▼端末２０は、メモリデバイス３０に格納されたカタログ情報を参照する。

▲４▼端末２０は、メモリデバイス３０からカタログ情報に対応するコンテンツデータの読み出しを行う。

▲５▼メモリデバイス３０は、エラー報告を端末２０に返す。

▲６▼端末２０は、コンテンツデータをサーバ１０に要求し、サーバ１０は端末２０にコンテンツを配信する。

▲７▼端末２０は、メモリデバイス３０の非耐タンパのメモリ領域にコンテンツデータを書き込む。

▲８▼メモリデバイス３０は、データの破損チェックを行いながら、コンテンツデータを端末２０に読み出す。

なお、▲１▼において、カタログ情報と検査情報とは、あらかじめメモリデバイス内に格納されていても良い。また、▲２▼において、カタログ情報は非耐タンパのメモリ領域に格納しても良い。

このように、このシステムでは、データ本体が必要になるまでデータ本体の配信を遅らせることができる。

また、このシステムでは、配信したコンテンツのデータが破損したとき、端末は、検査情報を基に、コンテンツデータを自動復元することができる。そのため、この検査情報を販売することにより、コンテンツデータの破損時に自動復元可能なコンテンツ配信サービスを提供したり、データ補修を目的とするサービスを提供したりすることが可能になり、新たなビジネスが成立する。

なお、各実施形態では、メモリデバイスが、外部からのトリガー（検査要求、読み出し要求）によって、データ破損の検査を行う場合について説明したが、メモリコントローラが自発的に（例えば、一定の周期で）データ破損の検査を行い、データが破損している場合に、その検査結果を外部に報告するようにしても良い。

また、各実施形態では、メモリデバイスに格納するデータ及び検査情報をサーバからダウンロードする場合について説明したが、このデータ及び／または検査情報は、メモリデバ

イスの製造時や配付時に書き込んでも良い。
また、各実施形態では、データをブロック単位で検査する場合について説明したが、本発明はブロック単位に限定されるものではない。
また、本発明におけるメモリデバイスには、カード形態のものだけでなく、ハードディスクなど、その他の形態の記憶装置も含まれる。
以上の説明から明らかなように、本発明のメモリデバイスは、検査情報を耐タンパ性の蓄積領域に格納し、データ本体を非タンパ性の蓄積領域に格納しているため、全ての情報を耐タンパ性の蓄積領域に格納する場合に比べて、多くのデータを格納することができ、また、低コストでの製造が可能になる。また、データ本体が破損した場合でも、耐タンパ性の蓄積領域に格納した検査情報を用いてデータ破損を確実に検出し、完全に修復することができる。
また、本発明のシステムでは、メモリデバイスに蓄積したデータが破損しているとき、正常データを外部から取得して修復するので、メモリデバイス内でバックアップ用のデータを重複して保持する必要が無く、メモリデバイスの蓄積効率を高めることができる。また、検査情報の生成単位を、データ全体ではなく、ブロック単位としているため、データ破損個所を小さな範囲に限定することができ、修復用の正常データを外部から取得する際のデータ通信時間を短縮することができる。
また、本発明のデータ修復システムの機能を利用して、データ本体が必要になるまでデータ本体の配信を遅らせるコンテンツ配信サービスを提供したり、コンテンツデータの破損時に自動復元可能なコンテンツ配信サービスを提供したり、あるいは、データ補修を目的とするサービスを提供したりすることができ、新たなビジネスの展開が可能になる。
本明細書は、２００２年１月３１日出願の特願２００２－０２３７０４に基づくものである。この内容をここに含めておく。
産業上の利用可能性
本発明は、例えば、端末装置の処理を規定するプログラムなどのデータを、サーバからネットワークを通じて端末装置にダウンロードするシステムに用いるに好適である。
【図面の簡単な説明】
図１は、本発明の実施の形態１におけるデータ修復システムの全体構成を示す図、
図２は、本発明の実施の形態１におけるメモリデバイスのハードウェア構成を示す図、
図３は、本発明の実施の形態１における検査情報の第１のデータ構成例を示す図、
図４は、本発明の実施の形態１における検査情報の第２のデータ構成例を示す図、
図５は、本発明の実施の形態１におけるメモリデバイスのデータ処理動作を示す図、
図６は、本発明の実施の形態１におけるメモリデバイスの書き込み手順を示すフロー図、
図７は、本発明の実施の形態１におけるメモリデバイスのデータ破損検査を伴う書き込み手順を示すフロー図、
図８は、本発明の実施の形態１におけるメモリデバイスのデータ破損検査手順を示すフロー図、
図９は、本発明の実施の形態１におけるメモリデバイスのデータ修復処理動作を示す図、
図１０は、本発明の実施の形態１におけるデータ修復システムでの修正情報取得動作を示す図、
図１１は、本発明の実施の形態１におけるメモリデバイスの修正データ書き込み手順を示すフロー図、
図１２は、本発明の実施の形態１におけるメモリデバイスのデータ読み出し手順を示すフロー図、
図１３は、本発明の実施の形態２におけるメモリデバイスのハードウェア構成を示す図、
図１４は、本発明の実施の形態２におけるメモリデバイスの暗号化データに対する処理動作１を示す図、
図１５は、本発明の実施の形態２におけるメモリデバイスの暗号化データに対する処理動作２を示す図、
図１６は、本発明の実施の形態３におけるメモリデバイスの署名付き検査情報の書き込み

動作を示す図、
図１７は、本発明の実施の形態３におけるメモリデバイスの暗号通信路で伝送された検査情報の書き込み動作を示す図、
図１８は、本発明の実施の形態４におけるメモリデバイスの署名付き検査情報の書き込み動作を示す図、
図１９は、本発明の実施の形態４におけるメモリデバイスの署名無し検査情報の書き込み動作を示す図、
図２０は、本発明の実施の形態５におけるメモリデバイスのデータ処理動作を示す図、及び、
図２１は、本発明の実施の形態５におけるシステムでのコンテンツ配信動作を示す図である。

【図１】

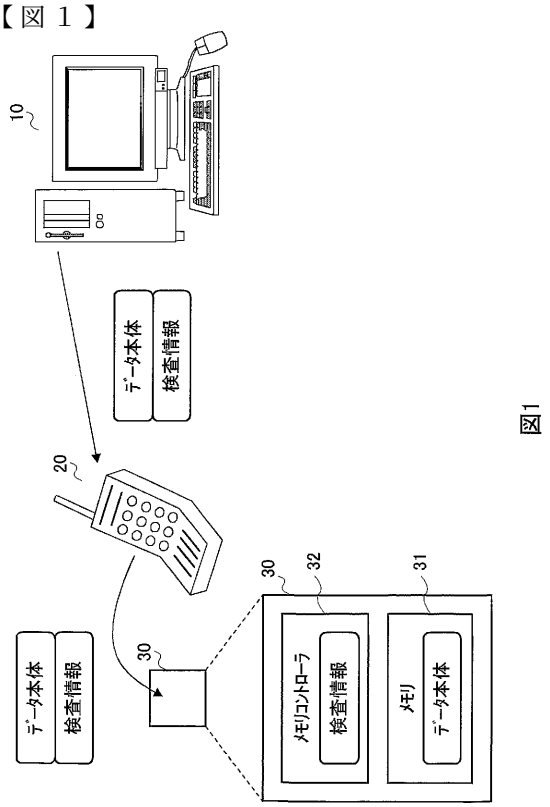


図1

【図２】

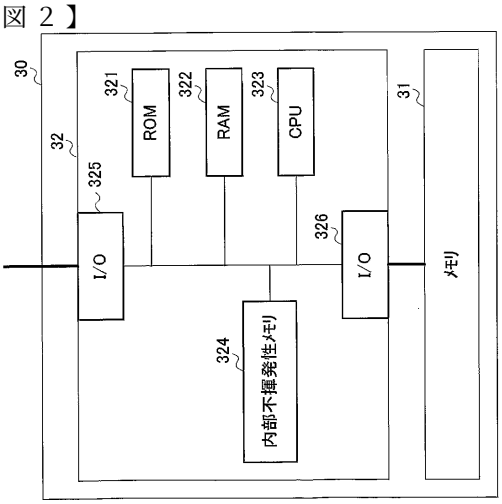


図2

【図３】

ファイル名
発行元
ファイルサイズ
ブロックサイズ
ハッシュ1
ハッシュ2
・・・

図3

【図４】

発行元	
データサイズ	
ブロックサイズ	
ブロック番号1	ハッシュ1
ブロック番号2	ハッシュ2
・・・	・・・

図4

【図５】

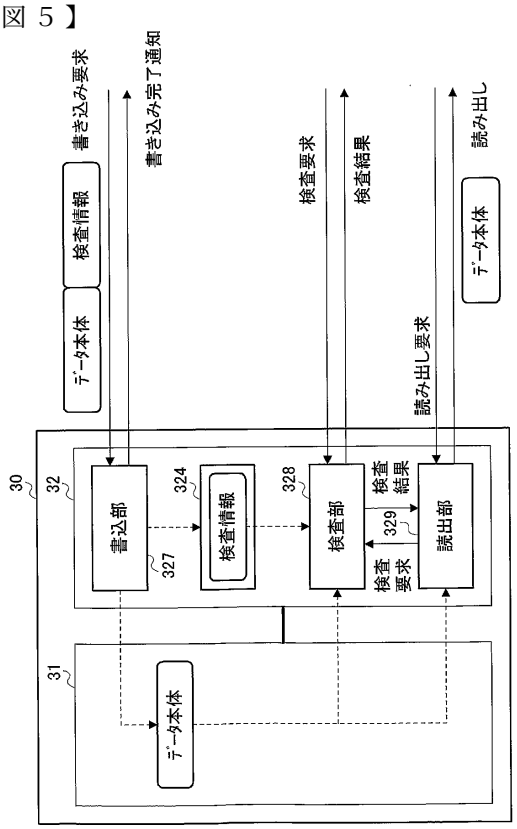


図5

【図６】

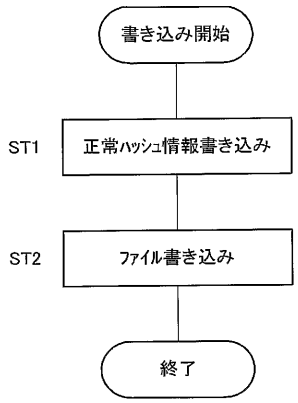


図6

【図７】

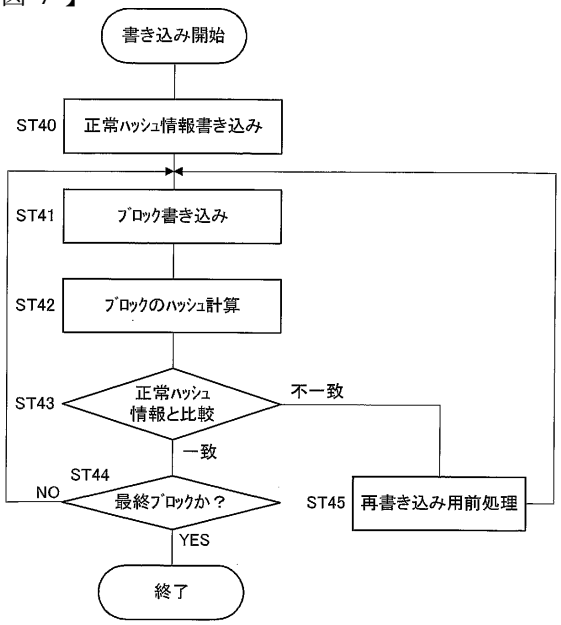


図7

【図８】

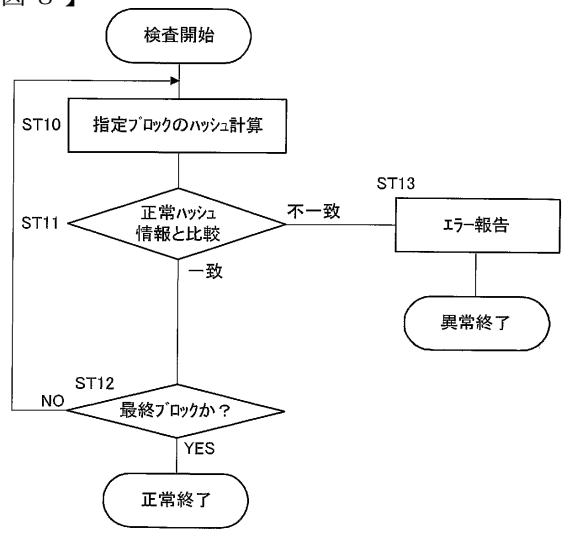


図8

【図９】

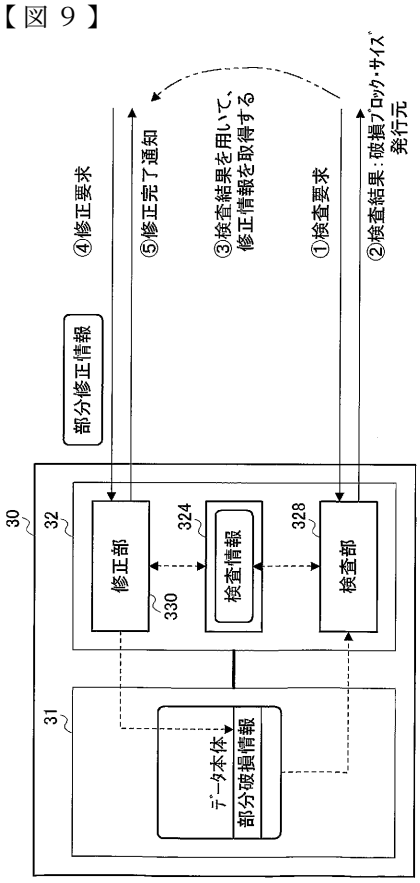


図9

【図１０】

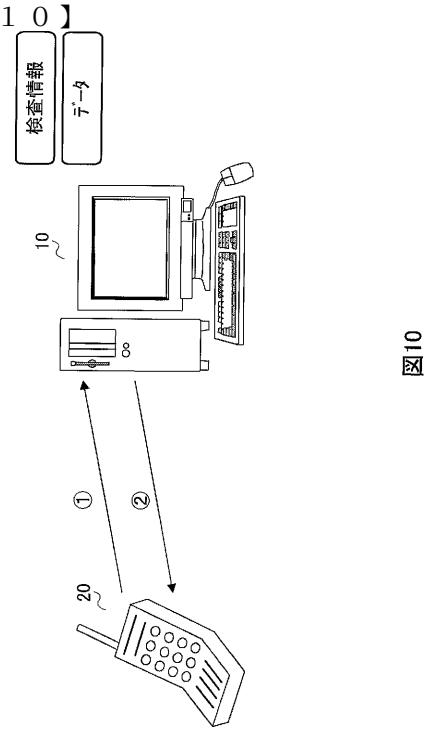


図10

【図１１】

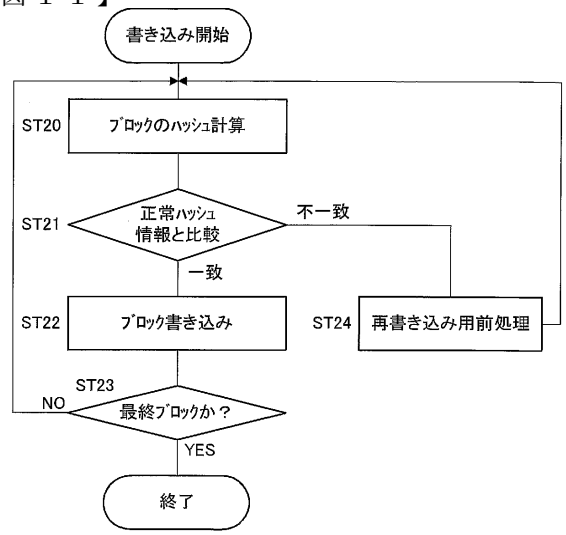


図11

【図１２】

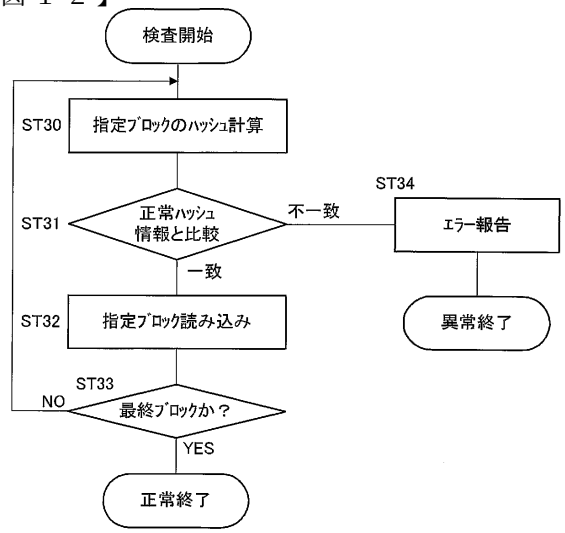


図12

【図１３】

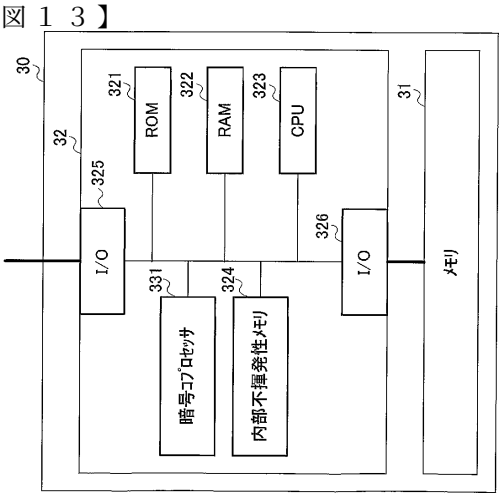


図13

【図１４】

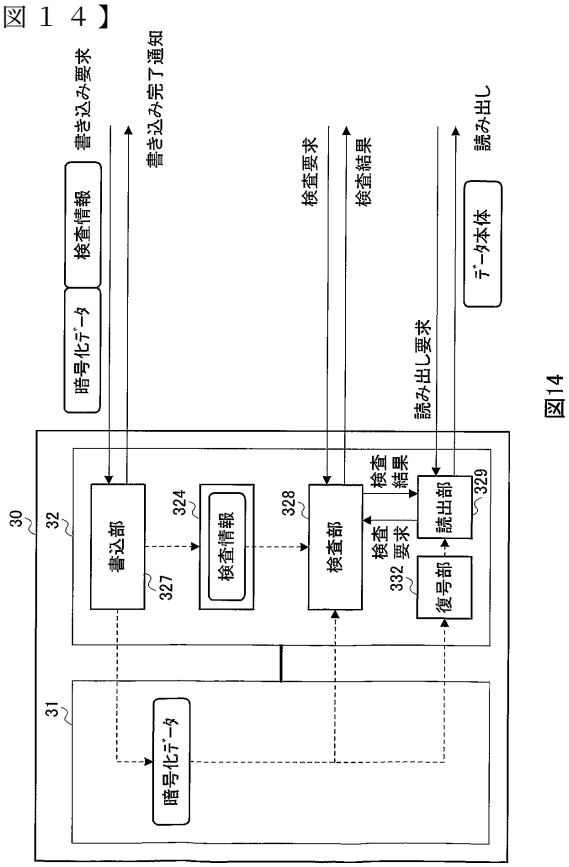


図14

【図１５】

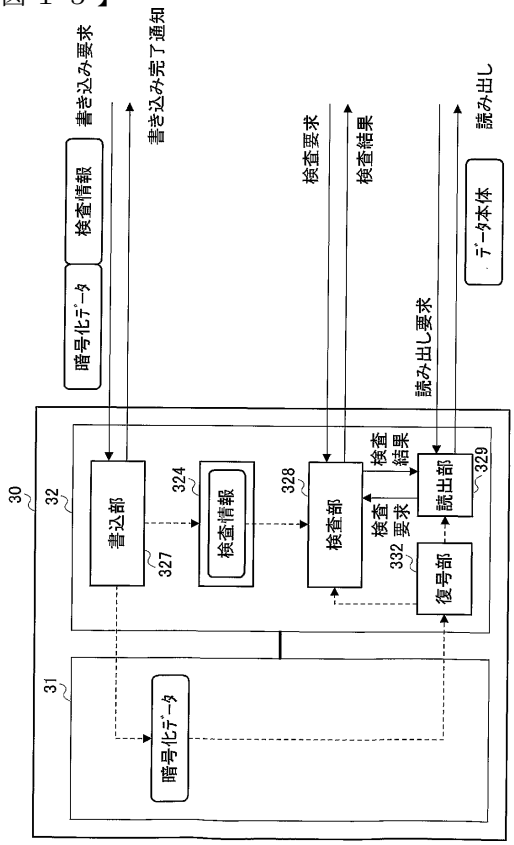


図15

【図１６】

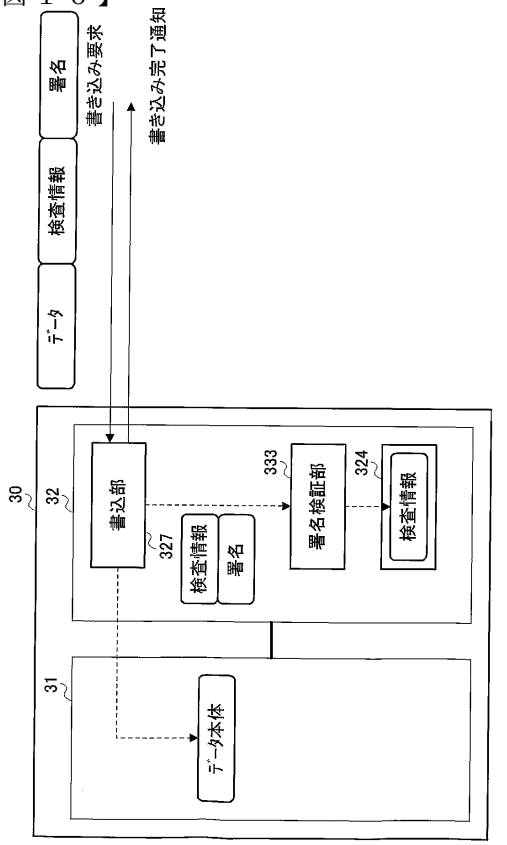


図16

【図１７】

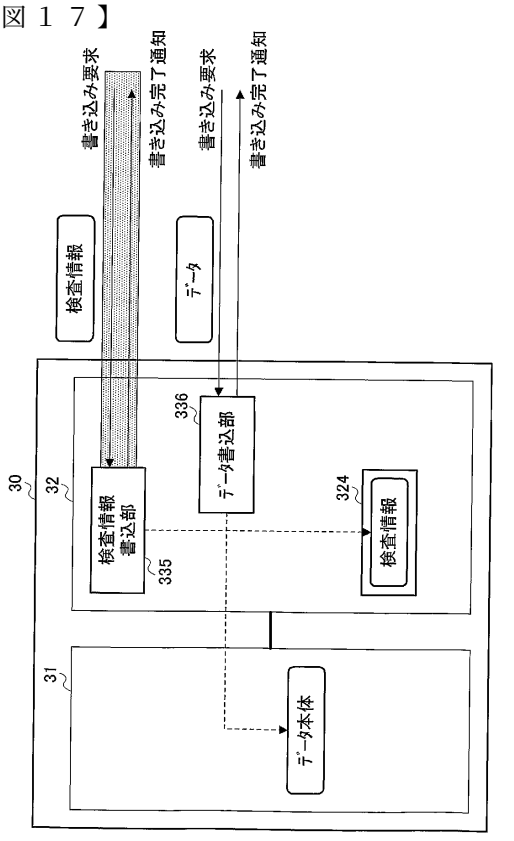


図17

【図１８】

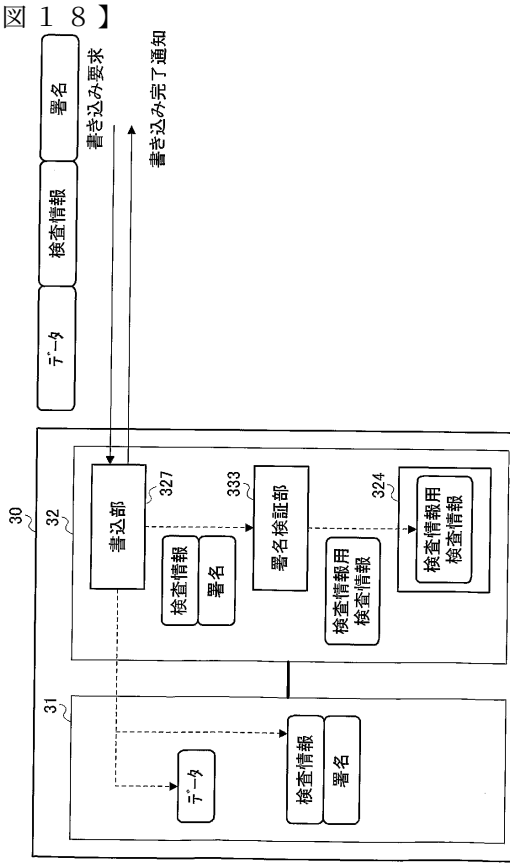


図18

【図１９】

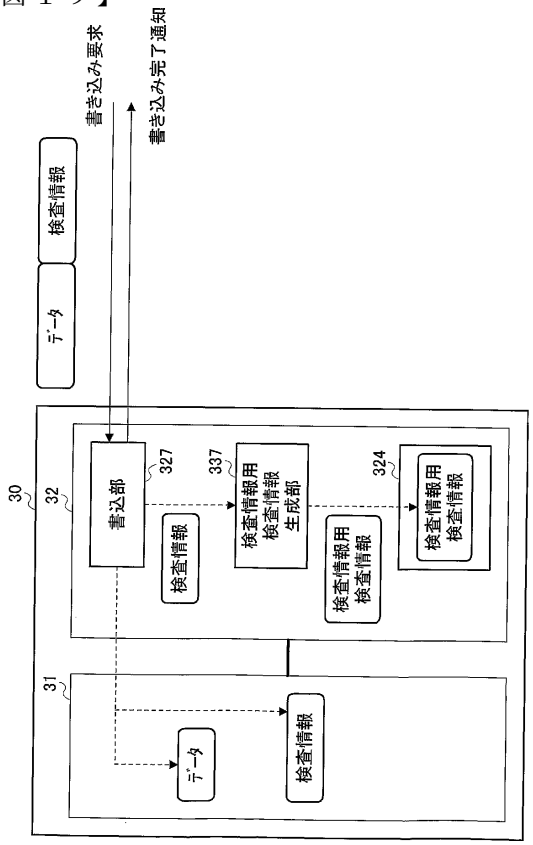


図19

【図２０】

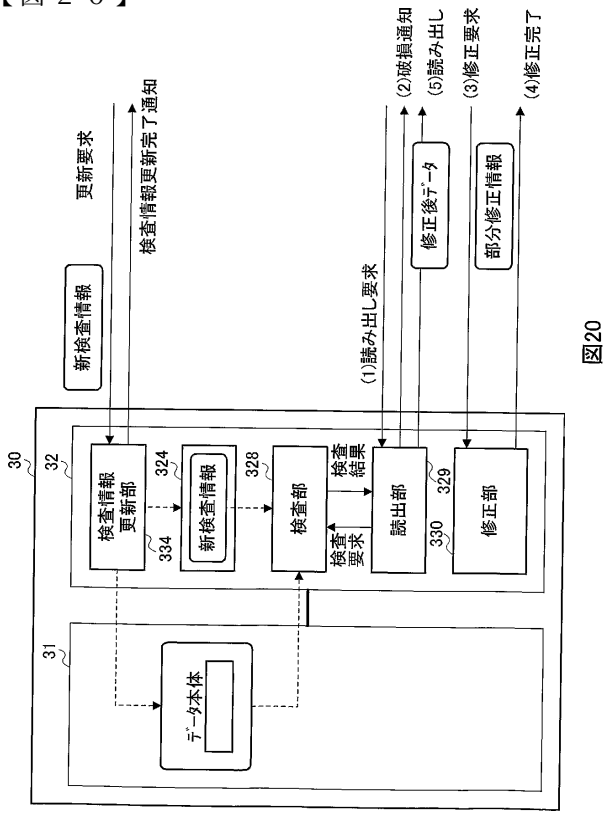


図20

【図２１】

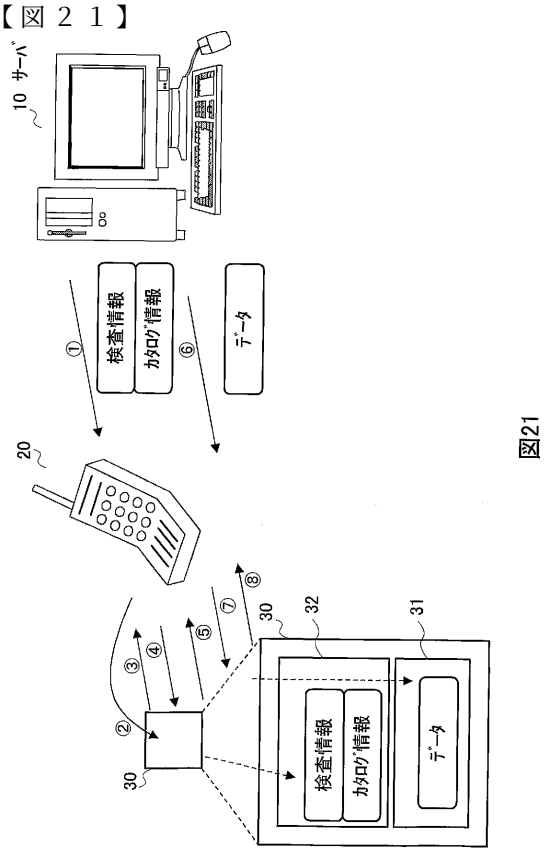


図21

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00500

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F12/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F12/16, G06F9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Toroku Jitsuyo Shinan Koho 1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 11-289526 A (Toshiba Corp.), 19 October, 1999 (19.10.99), Column 4, line 40 to column 6, line 18; Fig.2 (Family: none)	1-5,9,18-25 6-8,10-17
Y	JP 2001-290648 A (Hitachi, Ltd.), 19 October, 2001 (19.10.01), Full text; all drawings (Family: none)	1-5,9,18-25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 April, 2003 (11.04.03)	22 April, 2003 (22.04.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00500

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature common to claims 1-37 relates to "a memory device having a tamper-resistant memory area and a non-tamper-resistant memory area and storing data in the non-tamper-resistant memory area and inspection information to be used for inspection of data damage in the tamper-resistant memory area". However, the search has revealed that this technical feature is not novel since it is disclosed in document JP 11-289526 A (Toshiba Corporation), 1999.10.19, column 4, line 40 - column 6, line 18.

As a result, the technical feature makes no contribution over the prior art and cannot be a special technical feature within the meaning of PCT

(continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.: 1-25

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00500

Continuation of Box No.II of continuation of first sheet(1)

Rule 13.2, second sentence.

Consequently, there exists no technical feature common to claim 1, claims 2-25, claim 26, claims 27-31, claim 32, claims 33-34, claim 35, claim 36, and claim 37.

国際調査報告

国際出願番号 PCT／JP03／00500

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl.[7] G06F12／14, G06F12／16

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl.[7] G06F12／14, G06F12／16, G06F9／06

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2003年
日本国実用新案登録公報 1996－2003年
日本国登録実用新案公報 1994－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y A	JP 11－289526 A（株式会社東芝）1999.10.19, 第4欄, 第40行－第6欄, 第18行, 第2図（ファミリーなし）	1－5, 9, 18－25 6－8, 10－17
Y	JP 2001－290648 A（株式会社日立製作所）2001.10.19, 全文, 全図（ファミリーなし）	1－5, 9, 18－25

☐ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
11.04.03	22.04.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	堀江義隆	5N 9172
	電話番号 03－3581－1101 内線 3586	

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告	国際出願番号 PCT／JP03／00500

第Ⅰ欄 請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄 発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－３７に共通の事項は、「耐タンパ性のメモリ領域と非耐タンパ性のメモリ領域とを備え、前記非耐タンパ性のメモリ領域にデータを格納し、前記耐タンパ性のメモリ領域に前記データの破損の検査に用いる検査情報を格納したメモリデバイス」なる構成であるが、該構成は、文献ＪＰ １１－２８９５２６ Ａ（株式会社東芝），１９９９．１０．１９，第４欄第４０行－第６欄第１８行に開示されているから新規ではない。

結果として、上記構成は先行技術の域を出ないから、ＰＣＴ規則１３．２の第２文の意味において、この共通事項は特別な技術的特徴ではない。

それ故、請求の範囲１，２－２５，２６，２７－３１，３２，３３－３４，３５，３６，３７に共通の事項はない。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☒ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

請求の範囲１－２５

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。