

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4828155号
(P4828155)

(45) 発行日 平成23年11月30日(2011.11.30)

(24) 登録日 平成23年9月22日(2011.9.22)

(51) Int.Cl.

F I

H04L 9/32 (2006.01)
G06F 3/06 (2006.01)
G06F 21/24 (2006.01)
G06F 12/16 (2006.01)
G09C 1/00 (2006.01)

H04L 9/00 675A
 G06F 3/06 304R
 G06F 3/06 305A
 G06F 12/14 540A
 G06F 12/16 310C

請求項の数 5 (全 10 頁) 最終頁に続く

(21) 出願番号 特願2005-139227 (P2005-139227)
 (22) 出願日 平成17年5月12日(2005.5.12)
 (65) 公開番号 特開2006-319589 (P2006-319589A)
 (43) 公開日 平成18年11月24日(2006.11.24)
 審査請求日 平成20年4月3日(2008.4.3)

(73) 特許権者 000005108
 株式会社日立製作所
 東京都千代田区丸の内一丁目6番6号
 (74) 代理人 100093861
 弁理士 大賀 眞司
 (72) 発明者 水野 真喜夫
 神奈川県川崎市麻生区王禅寺1099番地
 株式会社日立製作所システム開発研究所
 内
 (72) 発明者 藤本 和久
 神奈川県川崎市麻生区王禅寺1099番地
 株式会社日立製作所システム開発研究所
 内
 審査官 石田 信行

最終頁に続く

(54) 【発明の名称】 ストレージシステム

(57) 【特許請求の範囲】

【請求項1】

外部装置と接続されるストレージシステムであって、
 前記外部装置より受信した第1のデータを暗号化し、該暗号化したデータを第2のデータとして復号化する第1の暗号復号部と、
 前記第1のデータを暗号化し、該暗号化したデータを第3のデータとして復号化する第2の暗号復号部と、
 前記第1のデータを暗号化し、該暗号化したデータを第4のデータとして復号化する第3の暗号復号部と、
 前記第2、第3及び第4のデータを比較する障害検出部を備え、
 前記障害検出部は、前記第2、第3及び第4のデータの中で不一致のデータがあれば、該不一致のデータを暗号化及び復号化した暗号復号部に障害が発生していると判断する、ストレージシステム。

【請求項2】

前記障害検出部は、前記第2、第3及び第4の暗号復号部のうち一つのみ結果が一致しない暗号復号部が存在する場合、当該暗号復号部に障害が発生していると判断する、請求項1記載のストレージシステム。

【請求項3】

前記障害検出部は、前記第2、第3及び第4のデータに基づいて、それぞれ第2、第3及び第4のハッシュ値を算出し、前記算出した第2、第3及び第4のハッシュ値を比較し

、前記算出した第2、第3及び第4のハッシュ値の中で一つのみ不一致のハッシュ値があれば、該不一致のハッシュ値が算出されたデータを暗号化及び復号化した暗号復号部に障害が発生していると判断する、請求項1記載のストレージシステム。

【請求項4】

外部装置と接続され、ディスク装置を備えるストレージシステムであって、
前記外部装置とのデータの送受信を行うチャンネルI/F部と、
前記外部装置から受信したデータを一時的に格納するメモリ部と、
前記ディスク装置とのデータの送受信を行うディスクI/F部を備え、
前記チャンネルI/F部と前記ディスクI/F部の少なくとも一つは、
前記外部装置より受信した第1のデータを暗号化し、該暗号化したデータを第2のデータとして復号化する第1の暗号復号部と、
前記第1のデータを暗号化し、該暗号化したデータを第3のデータとして復号化する第2の暗号復号部と、
前記第1のデータを暗号化し、該暗号化したデータを第4のデータとして復号化する第3の暗号復号部と、
前記第2、第3及び第4のデータを比較する障害検出部を備え、
前記障害検出部は、前記第2、第3及び第4のデータの中で不一致のデータがあれば、該不一致のデータを暗号化及び復号化した暗号復号部に障害が発生していると判断する、ストレージシステム。

【請求項5】

前記チャンネルI/F部は、前記障害検出部が、前記不一致のデータを暗号化及び復号化した暗号復号部に障害が発生していると判断した場合、前記外部装置に障害を報告する、請求項4記載のストレージシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データの暗号化及び復号化を行うストレージシステムに関する。

【背景技術】

【0002】

計算機等のセキュリティ対策の一つとして、データの暗号化技術がある（特許文献1参照）。暗号化を行う処理（以下、暗号処理と称する）、又は復号化を行う処理（以下、復号処理と称する）は、半導体部品やソフトウェアで実現されている。但し、半導体部品を用いると、 α 線等の放射線を受けることによる誤動作が考えられる。又、ソフトウェアを用いると、ある特定データパターンでの演算ミス等の障害が考えられる。

【0003】

一方、ストレージシステム自身のセキュリティ確保の要求が、近年、高まりつつある。一般に、サーバ等の外部装置は、ストレージシステムへデータを送信した時、当該データが正常にストレージシステムで受信されたことを確認するまで、当該データと同じデータを、当該外部装置のメインメモリ等に保持しておき、確認後、保持しておいたデータを削除する。又、ストレージシステムは、外部装置から送信されたデータを受信し、当該データを、自身の有するキャッシュメモリに一旦格納する。ストレージシステムは、当該データが正常に、自身の有するディスク装置へ格納されたことを確認すると、一定期間キャッシュメモリで保持するが、一定期間経過後、保持しておいたデータを削除する（特許文献2参照）。

【0004】

【特許文献1】特開2002-217887号公報

【特許文献2】特開平3-172946号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

10

20

30

40

50

以上の技術動向を鑑みると、今後は、上記ストレージシステムに、上記データ暗号化技術を適用することが考えられるが、単純に適用しただけでは、以下のような課題が生じる。

【0006】

ストレージシステムは、外部装置から受け取った、暗号化されていないデータ（以下、平文と称する）を暗号化して、当該暗号化したデータ（以下、暗号文と称する）を、ストレージシステム内のディスク装置に格納する。そして、ディスク装置に格納したデータを復号化して、当該復号化したデータ（以下、復号文と称する）を、外部装置に送信する。この際、平文と復号文は、外部装置から見れば当然同一でなければならないが、暗号処理、もしくは復号処理に失敗していた場合には、平文と復号文が同一とならない。

10

【0007】

例えば、復号処理に失敗（復号化処理回路や処理プログラムの障害等）した場合、正常に暗号処理された暗号文であれば、正常な復号処理を施すことにより（別の正常な復号化処理回路等を用いる）、当該暗号文を平文に戻すことは可能である。しかし、暗号処理に失敗していた場合には、最初に外部装置から送信された平文は、すでに削除されている可能性が高いため、復号処理は正常であったとしても、元の平文に戻すことはできない。即ち、外部装置から見れば復号文は無意味な単なる文字列であって、結果的にデータロスとなってしまう。

【課題を解決するための手段】

【0008】

上記課題を解決するために、本発明の一実施態様は以下の構成を有する。

20

【0009】

ストレージシステムは、外部装置より受信した第1のデータを暗号化する暗号部と、暗号化したデータを第2のデータとして復号化する復号部と、第1及び第2のデータを比較する比較部とを備える。第1及び第2のデータが不一致の場合、外部装置に障害を報告する。又は、第1のデータを暗号化した暗号部とは異なる暗号部で第1のデータを暗号化し、復号部で該暗号化したデータを第3のデータとして復号化し、第1及び第3のデータを比較してもよい。

【発明の効果】

【0010】

本発明によれば、暗号部の障害による復号文と平文の不一致を未然に防ぐことができる。

30

【発明を実施するための最良の形態】

【0011】

以下、本発明の実施形態について、図面を参照して説明する。

【0012】

図1は、計算機システムの構成例を示す図である。計算機システムは、ストレージシステム1、サーバ（計算機）3及び管理端末8とから構成される。ストレージシステム1とサーバ3とは、ネットワークを介して相互に接続される。

【0013】

ストレージシステム1は、サーバ3とのデータの送受信を行うチャンネルI/F部11、ディスク装置2とのデータの送受信を行うディスクI/F部16、スイッチ部51、メモリ部21、及びディスク装置2とから構成される。チャンネルI/F部11及びディスクI/F部16はスイッチ部51を介してメモリ部21に接続される。

40

【0014】

管理端末8は、ストレージシステム1内のチャンネルI/F部11及びディスクI/F部16内のマイクロプロセッサ（以下、MPと称する）にネットワークを介して接続される。管理端末8は、主に、ストレージシステム1の構成設定、監視、稼動情報・障害情報等の収集を行い、後述する暗号復号部の障害による平文と復号文の不一致も障害情報として収集する。管理端末8が収集した情報により、例えば、どの暗号復号部に障害が発生している

50

かということ把握できるため、交換対象の部品を容易に特定することが可能である。尚、管理端末 8 の機能は、サーバ 3 内、ストレージシステム 1 内、あるいは、ネットワーク上にあってもよく、本構成に限定されるものではない。

【0015】

又、本稿記載のネットワークは、IP ネットワーク、FC ネットワーク等が考えられるが、これらに限定されるものではない。

【0016】

チャンネル I F 部 1 1、ディスク I F 部 1 6 及びメモリ部 2 1 は、2 つのスイッチ部 5 1 と 1 本ずつの通信パスで各々接続される。ここで、通信パスとは、データ／制御情報を伝送するための単数又は複数の信号線から成る伝送路である。これにより、チャンネル I F 部 1 1、ディスク I F 部 1 6 及びメモリ部 2 1 のそれぞれの間で 2 つの通信経路を確保し、ストレージシステムの信頼性をあげることが可能となる。尚、上記個数や本数は一実施形態に過ぎず、上記に限定するものではない。このことは以下に説明する実施形態全てに当てはまる。又、本実施形態では、チャンネル I F 部 1 1、ディスク I F 部 1 6 及びメモリ部 2 1 との間を、スイッチ部 5 1 を介して接続する例を示したが、これらの各部を相互に接続してデータ／制御情報が転送されればよいのであり、例えばバスを介して各部位を相互に接続してもよい。

【0017】

メモリ部 2 1 は、メモリモジュール 1 2 7 及びメモリコントローラ 1 2 5 を有する。メモリモジュール 1 2 7 は論理的に 2 つの領域に分けられている。1 つの領域はキャッシュメモリ領域で、ディスク装置 2 に書き込まれるデータ又はディスク装置 2 から読み出されたデータが一時的に格納される領域である。もう 1 つの領域は制御メモリ領域で、チャンネル I F 部 1 1、ディスク I F 部 1 6 及びメモリ部 2 1 間のデータ転送を制御するための情報、ストレージシステム 1 の管理情報、並びに構成情報等が格納される領域である。メモリコントローラ 1 2 5 は、メモリモジュール 1 2 7 へのデータのリード／ライト処理を制御する。又、メモリコントローラ 1 2 5 は、チャンネル I F 部 1 1、ディスク I F 部 1 6 及び他のメモリ部 2 1 との間のデータ／制御情報の転送を制御する。

【0018】

一般に、ストレージシステムは、サーバ等の外部装置から受け取ったデータを、キャッシュメモリへ格納した後、ディスク装置に格納する。一つの方法として、キャッシュメモリへ格納したデータをディスク装置に格納した後、外部装置へデータ処理終了を報告する方法がある（キャッシュライトスルー）。別の方法として、キャッシュメモリへのデータ格納処理と、キャッシュメモリからディスク装置へのデータ格納処理を非同期に行う方法がある（キャッシュライトバック）。即ち、キャッシュメモリにデータを格納した時点で外部装置にデータ処理終了を報告し、その後、キャッシュメモリのデータをディスク装置へ格納する。全体の処理時間は、後者の方が前者よりも短くなる。

【0019】

尚、メモリモジュール 1 2 7 が物理的に 2 つのモジュール、即ち、キャッシュメモリモジュールと制御メモリモジュールに分かれていてもよい。この場合、メモリコントローラ 1 2 5 が、2 つのメモリモジュールへのデータのリード／ライト処理を独立に制御する。又、メモリコントローラ 1 2 5 がキャッシュメモリモジュール制御用と制御メモリモジュール制御用に分離されていてもよい。更に、ストレージシステム 1 の 2 つのメモリ部 2 1 間で、メモリモジュール 1 2 7 へ格納するデータ／制御情報を二重化（複製して双方に格納）してもよい。こうすることにより、1 つのメモリ部 2 1 に障害が発生した場合、もう一方のメモリ部 2 1 に格納されたデータで動作を継続することが可能となり、ストレージシステム 1 の信頼性が向上する。

【0020】

ディスク装置 2 は、一般に磁気ディスクであるが、光ディスク、半導体メモリ等、他の記憶媒体を用いたものであってもよい。又、ディスク装置 2 は、ディスクアレイのように複数のハードディスクドライブで構成されてもよいし、RAID 構成であってもよい。

【0021】

図2は、チャンネルIF部11の詳細を示す図である。

【0022】

チャンネルIF部11は、サーバ3とのデータ転送を制御するホストIF101、チャンネルIF部11を制御するMP100、メモリ部21との間のデータ／制御情報の転送を制御する転送制御部103、及び暗号復号部201（201-1、201-2）を有する。

【0023】

暗号復号部201は、暗号処理を行う暗号部202、復号処理を行う復号部203、比較部204、データの入出力を行う入出力部、暗号復号部201内で発生した障害回数をカウントするカウンタ207、及び障害回数の閾値を設定するレジスタ208を有する。入出力部は、転送制御部103側を入出力部205、スイッチ部51側を入出力部206とする。

10

【0024】

ホストIF101は、共通バス104を介して転送制御部103に接続される。又、MP100は、共通バス105を介して転送制御部103に接続される。更に、データ転送制御部103は、暗号復号部201を介して2つのスイッチ部51と接続するための通信バス106を2本有する。暗号復号部201は、通信バス106毎に設ける。これにより、通信バス106毎に暗号及び復号処理を実施できるため、通信バス106間の競合を避けることができる。しかし、部品コスト削減のために単一の暗号復号部であってもよい。

【0025】

20

MP100は、メモリモジュール127内の制御メモリ領域に格納された制御情報に基づいて、メモリモジュール127内のキャッシュメモリ領域へのデータのリード／ライト処理、キャッシュメモリ領域のディレクトリ管理、及びホストIF101とメモリ部21との間のデータ転送を制御する。又、後述のように、暗号文と復号文との比較結果のチェック、及び暗号文と復号文が不一致の場合のサーバ3や管理端末8等への障害報告等の処理を行う。

【0026】

ここで、ホストIF101、MP100、暗号復号部201、及び転送制御部103の間の接続構成は一実施形態に過ぎず、構成を上記に限定するものではない。少なくとも、ホストIF101からメモリ部21へデータ転送するまでに、転送制御部103、暗号復号部201を通過する構成であればよい。又、MP100がホストIF101及び転送制御部103を制御でき、メモリ部21へアクセスできる構成であればよい。更に、少なくとも、暗号部202、復号部203、及び比較部204があればよく、暗号復号部201として、これらを括らなくともよい。更に、後述のように、暗号及び復号処理をディスクIF部16のみに行わせる場合は、暗号復号部201はなくてもよい。更に、データの送受信を行う相手は、サーバ3に限られず、ストレージシステム1に接続される外部装置であれば何でもよい。例えば、リモートコピーを行う場合には、相手が他のストレージシステムとなることもある。

30

【0027】

図3は、暗号処理のフロー図である。

40

【0028】

暗号復号部201-1において、MP100は、サーバ3等から送信された平文を、ホストIF101、転送制御部103を経て入出力部205から暗号部202と比較部204に入力する（ステップ301）。比較部204では平文を保持しておく。次に、暗号部202は、入力された平文を暗号化し、暗号部202で該暗号文を保持すると共に、該暗号文を復号部203へ渡す（ステップ302）。次に、復号部203は、渡された暗号文を復号化し、該復号文を比較部204へ渡す（ステップ303）。次に、比較部204は、保持しておいた平文と、復号部203から渡された復号文を比較する（ステップ304）。MP100は、その結果をチェックし（ステップ305）、両者が一致していれば、正しく暗号化されたと判断し、暗号部202で保持しておいた暗号文を、スイッチ部51

50

を介してメモリ部 21 へ送信する（ステップ 306）。一致していなければ、MP100は、正しく暗号化されなかったと判断し、比較部 204 で保持しておいた平文を暗号復号部 201-2 に送信し、暗号復号部 201-2 で処理をやり直す（ステップ 307）。ここで一致すれば、ステップ 306 の処理を行い、一致しなければ、サーバ 3 や管理端末 8 等に当該障害を報告する（ステップ 308）。

【0029】

尚、暗号復号部 201-1 内の暗号部 202 等の回路は、通常は正常に動作していても、まれに誤動作を起こすことがあり得る。逆に言えば、一回誤動作を起こしたからといって、当該回路に障害が発生しているとは限らない。そこで、一定回数以上誤動作を起こした場合に障害が発生していると判断する、という処理を追加してもよい。まず、レジスタ 208 に障害発生回数の閾値を予め設定しておく。カウンタ 207 は、障害発生回数をカウントし、その値が、閾値を超えた時点で、MP100 は、処理を暗号復号部 201-2 に切り替える。暗号復号部 201-2 においても閾値を超えれば、MP100 は、サーバ 3 や管理端末 8 等に障害を報告する。

10

【0030】

又、暗号復号部 201 の個数は上記に限定されるものではなく、例えば、n 個ある場合には、n 個の暗号復号部 201 が処理を行うこともあり得る。n 個の暗号復号部 201 の全てに障害が発生していた場合に、MP100 が障害を報告してもよいし、一定個数に障害が発生していた場合に、障害を報告するようにしてもよい。

【0031】

20

更に、後述のように、ディスク I/F 部 16 で暗号及び復号処理を行う場合は、ステップ 306 で（例えば、一定個数の暗号復号部 201 に障害が発生していると判断した時点）、当該暗号文ではなく当該平文をメモリ部 21 に転送してもよく、最終的にディスク装置 2 に格納するときに暗号文になっていればよい。

【0032】

ここで、平文や復号文などのデータ自体を比較する方法以外に、そのデータからある一定の法則に基づいて算出する固定長の値を用いた方法もある。この固定長の値は、ハッシュ値と呼ばれる（メッセージダイジェストとも呼ばれる）。ハッシュ値は、元のデータの微妙な違いから、データ毎に全く異なる値となる。この性質を平文と復号文の比較に用いる。図 3 の暗号処理のフロー図に当てはめると、ステップ 301 で平文を比較部 204 に入力した後に、比較部 204 はハッシュ値 1 を算出し、ステップ 303 で復号文からハッシュ値 2 を算出し、ステップ 304 でハッシュ値 1 とハッシュ値 2 を比較する。そして、ステップ 305 で MP100 が結果をチェックする。

30

【0033】

尚、サーバ 3 等が本処理で用いた暗号復号部と同じ機能を保持している場合は、ステップ 301 にて、サーバ 3 等から暗号文としてデータが送信されてくることもあり得る。この場合は、もともと暗号化されているため、暗号部 202 が正常か否かのチェックを行う必要はない。しかし、後述のような復号処理を行うことにより、復号部 203 が正常か否かを判断したり、一旦、復号化した後、上記暗号処理により、暗号部 202 が正常か否かの判断をしてもよい。

40

【0034】

サーバ 3 等と暗号文のやりとりを行う場合には、サーバ 3 等が用いる暗号鍵を取得しなければならない。そこで、サーバ 3 等と予め暗号鍵を交換しておくか、外部に認証サーバ等を設けることになる。

【0035】

図 4 は、復号処理のフロー図である。

【0036】

暗号復号部 201-1 において、MP100 は、暗号文をメモリ部 21 から読み出し、入出力部 206 から復号部 203 と比較部 204 に入力する（ステップ 401）。ここで、復号対象の暗号文がメモリ部 21 に存在しない場合、ディスク I/F 部 16 がディスク装置

50

2 から暗号文を読み出し、メモリ部 2 1 へ書き込んだ後で、MP 1 0 0 がメモリ部 2 1 から暗号文を読み出す。比較部 2 0 4 では暗号文を保持しておく。次に、復号部 2 0 3 は、入力された暗号文を復号化し、復号部 2 0 3 で該復号文を保持すると共に、該復号文を暗号部 2 0 2 へ渡す（ステップ 4 0 2）。次に、暗号部 2 0 2 は、渡された復号文を暗号化し、該暗号文を比較部 2 0 4 へ渡す（ステップ 4 0 3）。次に、比較部 2 0 4 は、保持しておいた暗号文と、暗号部 2 0 2 から渡された暗号文とを比較する（ステップ 4 0 4）。MP 1 0 0 は、その結果をチェックし（ステップ 4 0 5）、両者が一致していれば、正しく復号化されたと判断し、復号部 2 0 3 で保持しておいた復号文を、転送制御部 1 0 3、ホスト I F 1 0 1 を介してサーバ 3 に送信する（ステップ 4 0 6）。一致していなければ、MP 1 0 0 は、正しく復号化されなかったと判断し、比較部 2 0 4 で保持しておいた暗号文を暗号復号部 2 0 1 - 2 に送信し、暗号復号部 2 0 1 - 2 で処理をやり直す（ステップ 4 0 7）。ここで一致すれば、ステップ 4 0 6 の処理を行い、一致しなければ、サーバ 3 や管理端末 8 等に当該障害を報告する（ステップ 4 0 8）。暗号復号部 2 0 1 の個数を n 個とした場合の処理は、暗号処理のフローと同様である。尚、サーバ 3 等が本処理で用いた暗号復号部と同じ機能を保持している場合は、ステップ 4 0 6 にて、チェックの終わった暗号文をそのまま、サーバ 3 等へ送信してもよい。

10

【0037】

ここで、暗号処理時と同様、ハッシュ値を用いて比較してもよい。図 4 の復号処理のフロー図に当てはめると、ステップ 4 0 1 で暗号文を比較部 2 0 4 に入力した後に、比較部 2 0 4 はハッシュ値 1 を算出し、ステップ 4 0 3 で暗号文からハッシュ値 2 を算出し、ステップ 4 0 4 でハッシュ値 1 とハッシュ値 2 を比較する。そして、ステップ 4 0 5 で MP 1 0 0 が結果をチェックする。

20

【0038】

本実施例では、データ自体を比較する方法及びハッシュ値を用いて比較する方法を記載したが、比較する方法は、これらに限定されるものではない。

【0039】

上記暗号及び復号処理は、ディスク I F 部 1 6 で行ってもよい。例えば、暗号処理を行うタイミングは、サーバ 3 から受信したデータが一旦メモリモジュール 1 2 7 に格納され、該データがディスク装置 2 に格納される時点である。ディスク I F 部 1 6 の構成は、ほぼチャンネル I F 部 1 1 と同様なので図示を省略するが、チャンネル I F 部 1 1 との違いは、ホスト I F 1 0 1 がサーバ 3 等の外部装置との間のデータ転送を制御するのに対して、ホスト I F 1 0 1 に相当する部分（ディスク I F）は、スイッチ部 5 1 を介してメモリ部 2 1 との間のデータ転送を制御する。又、チャンネル I F 部 1 1 の入出力部 2 0 6 は、スイッチ部 5 1 を介してメモリ部 2 1 と接続されるが、ディスク I F 部 1 6 の該入出力部は、ディスク装置 2 に接続される。

30

【0040】

以上に説明した処理は、チャンネル I F 部 1 1 及びディスク I F 部 1 6 の両方で行ってもよいし、どちらか一方のみで行ってもよい。即ち、暗号処理はチャンネル I F 部 1 1 のみで行い、復号処理はディスク I F 部 1 6 のみで行う等、様々なバリエーションが考えられる。バリエーションによって、ステップ 3 0 6 及び 4 0 6 の処理が変わることがある。例えば、暗号処理をチャンネル I F 部 1 1 及びディスク I F 部 1 6 の両方で行う場合は、チャンネル I F 部 1 1 は、ステップ 3 0 6 において、平文をメモリ部 2 1 へ送信することとなる（ディスク I F 部 1 6 が暗号文をディスク装置 2 へ送信する）。又、復号処理をチャンネル I F 部 1 1 及びディスク I F 部 1 6 の両方で行う場合は、ディスク I F 部 1 6 は、ステップ 4 0 6 において、暗号文をメモリ部 2 1 へ送信することとなる（チャンネル I F 部 1 1 が復号文をサーバ 3 へ送信する）。

40

【0041】

以上の実施例では、暗号部 2 0 2 と復号部 2 0 3 を独立の論理回路であるとして説明したが、これらを一体化した論理回路である暗号復号部としてもよい。但し、この場合に障害が発生すると、暗号化及び復号化を備える機能が共に影響を受けるため、先述のような

50

処理を行うと、見た目は平文と、暗号化し復号化した復号文は一致してしまう。これでは暗号復号部の障害を検出することができない。

【0042】

そこで、暗号復号部を複数用意し、更に、暗号復号部の障害を検出する障害検出部を設ける。障害検出部は、暗号及び復号処理を別々の暗号復号部でそれぞれ実施させた結果が一致しなければ、少なくともどちらかの暗号復号部に障害が生じていると判断する。又、3つ以上の暗号復号部を用いた場合、一つのみ結果が一致しない暗号復号部が存在すれば、当該一致しない暗号復号部に障害が発生していると判断する。そして、MPがサーバや管理端末等の外部装置に障害を報告する。尚、上記同様に、カウンタを設けて、一定回数以上誤動作を起こした場合に障害を報告するようにしてもよい。

10

【0043】

以上の実施例では、暗号部、復号部、比較部、暗号部と復号部を一体化した暗号復号部及び障害検出部等はハードウェアであるかのように説明したが、これらをプログラムで実現してもよい。例えば、チャンネルIF部11内にプログラムを格納するメモリを用意し、当該メモリに暗号プログラム、復号プログラム、比較プログラム等を格納し、それらのプログラムをMPが実行することにより、以上で説明したような処理を実現できる。これはディスクIF部でも同様に実現できる。こうしたプログラムは、計算機による読み取り可能な記憶媒体(CD-ROM等)に記憶して提供することが可能である。又、これらのプログラムを、インターネット等のネットワークを通して提供することも可能である。

【図面の簡単な説明】

20

【0044】

【図1】 計算機システムの構成例を示す図。

【図2】 チャンネルIF部の構成例を示す図。

【図3】 暗号処理のフロー図。

【図4】 復号処理のフロー図。

【符号の説明】

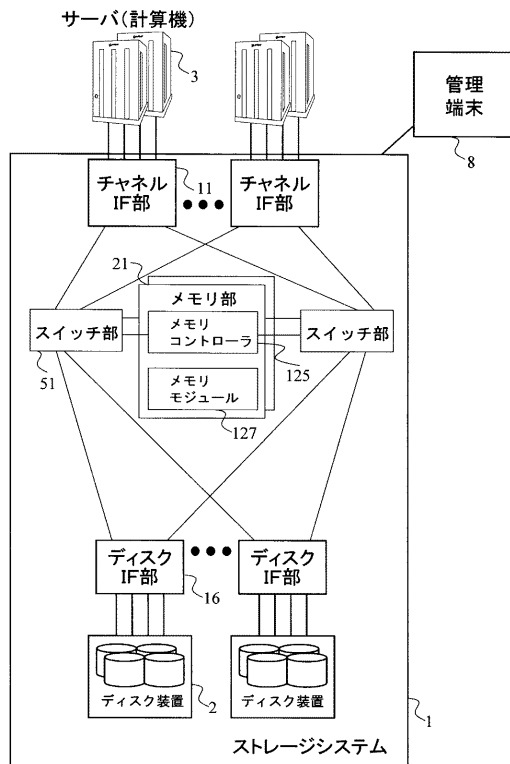
【0045】

1…ストレージシステム、2…ディスク装置、3…サーバ、4…チャンネルIF、5…ディスクIF、6…メモリ部、7…スイッチ部、100…マイクロプロセッサ、101…ホストIF、102…ディスクIF、103…転送制御部、125…メモリコントローラ、127…メモリモジュール、201…暗号復号部、202…暗号部、203…復号部、204…比較部、205、206…入出力部、207…カウンタ、208…レジスタ。

30

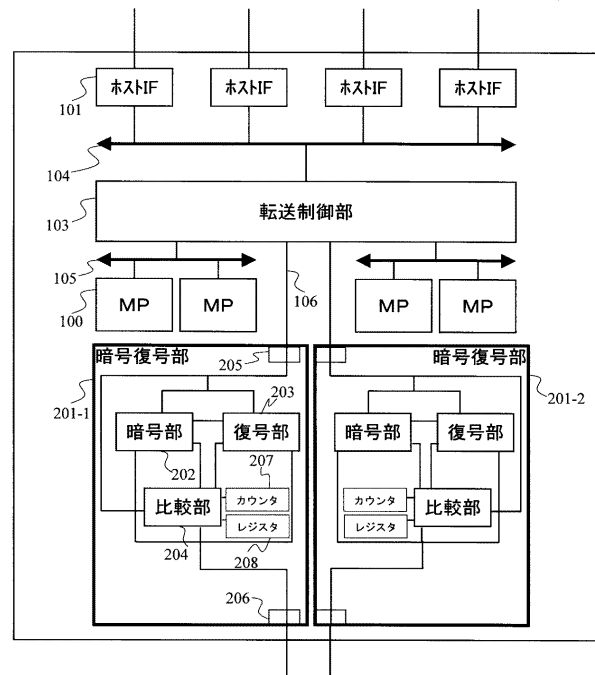
【図 1】

図1



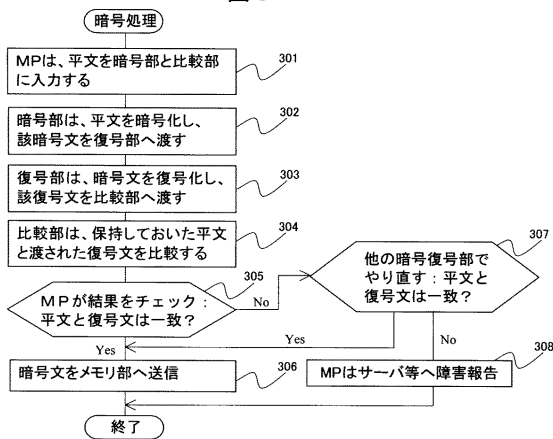
【図 2】

図2



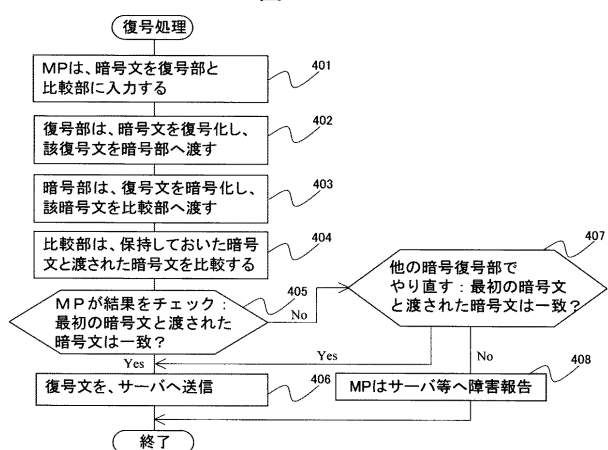
【図 3】

図 3



【図 4】

図 4



フロントページの続き

(51)Int.Cl.			F I		
H04L	9/10	(2006.01)	G06F	12/16	310H
			G09C	1/00	640D
			H04L	9/00	621A

(56)参考文献 特開2004-295273 (JP, A)
特開平01-099341 (JP, A)
特開平11-305659 (JP, A)
特開2003-209546 (JP, A)
特開2006-042108 (JP, A)
特開2005-341422 (JP, A)
特開2001-331380 (JP, A)
特開2001-216196 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L	9/32
H04L	9/10
G09C	1/00
G06F	3/06
G06F	12/16
G06F	21/24