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

特許第4728060号
(P4728060)

(45)発行日　平成23年7月20日(2011.7.20)　(24)登録日　平成23年4月22日(2011.4.22)

(51)Int.Cl.		F I		
H04L 9/14	(2006.01)	H04L	9/00	641
G06F 3/06	(2006.01)	G06F	3/06	304H
G11B 20/12	(2006.01)	G11B	20/12	
G11B 20/10	(2006.01)	G11B	20/10	H
		G11B	20/10	301Z

請求項の数 8　(全 30 頁)

(21)出願番号　特願2005-211247(P2005-211247)
(22)出願日　平成17年7月21日(2005.7.21)
(65)公開番号　特開2007-28502(P2007-28502A)
(43)公開日　平成19年2月1日(2007.2.1)
審査請求日　平成20年1月9日(2008.1.9)

(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　100075513
弁理士　後藤　政喜
(74)代理人　100084537
弁理士　松田　嘉夫
(74)代理人　100114236
弁理士　藤井　正弘
(72)発明者　藤林　昭
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】ストレージ装置

(57)【特許請求の範囲】
【請求項１】
ネットワークを介してホスト計算機と接続するホストインターフェース部と、
ディスク装置と接続するディスクインターフェース部と、
ストレージ装置の制御情報を格納し、キャッシュメモリとして機能するメモリ部と、
ストレージ装置を制御するプロセッサ部と、
前記ホストインターフェース部、前記ディスクインターフェース部、前記メモリ部及び前記プロセッサ部を相互に接続する相互結合部と、
前記ホスト計算機によって読み書きされるデータを暗号化する暗号化機能部と、
を備え、
前記ディスク装置には第１の論理ボリューム及び第２の論理ボリュームが設定されており、
前記第１の論理ボリュームと前記第２の論理ボリュームとでコピーペアが設定されており、
前記プロセッサ部は、
前記第１の論理ボリュームに格納されているデータを読み出し、
前記読み出されたデータを、当該第１の論理ボリュームに対応する暗号鍵を用いて復号化し、
前記復号化されたデータを、前記第２の論理ボリュームに対応する暗号鍵を用いて暗号化し、

前記暗号化されたデータを前記第２の論理ボリュームに書き込むことによって、前記第１の論理ボリュームの内容を前記第２の論理ボリュームに複製し、
前記ホスト計算機から前記第１の論理ボリュームへのデータの書き込み要求があった場合は、当該書き込みデータを前記第１の論理ボリュームに対応する暗号鍵を用いて暗号化し、暗号化されたデータを前記第１の論理ボリューム及び第２の論理ボリュームに書き込み、
前記コピーペアの状態が変化した場合は、前記第１の論理ボリュームに対応する暗号鍵を変更し、当該変更した暗号鍵を用いて前記書き込みデータを暗号化し、暗号化されたデータを前記第１の論理ボリュームに書き込むことを特徴とするストレージ装置。
【請求項２】
前記プロセッサ部は、データを暗号化又は復号化するときに、当該データを、前記暗号化機能部に送信することを特徴とする請求項１に記載のストレージ装置。
【請求項３】
前記プロセッサ部は、データを暗号化又は復号化するときに、当該データを、前記メモリ部のキャッシュメモリ領域に書き込むことを特徴とする請求項１に記載のストレージ装置。
【請求項４】
前記ホスト計算機がデータの書き込みを要求した場合に、
前記プロセッサ部は、
前記書き込みデータを前記メモリ部のキャッシュメモリ領域に格納し、
前記格納された書き込みデータを前記暗号化機能部に送信し、
前記暗号化機能部によって暗号化されたデータを、当該書き込み要求に係る領域に書き込むことを特徴とする請求項１に記載のストレージ装置。
【請求項５】
前記暗号化機能部は、前記ホストインターフェース部に備わることを特徴とする請求項１に記載のストレージ装置。
【請求項６】
前記暗号化機能部は、前記ディスクインターフェース部に備わることを特徴とする請求項１に記載のストレージ装置。
【請求項７】
前記暗号化機能部は、前記メモリ部に備わることを特徴とする請求項１に記載のストレージ装置。
【請求項８】
ネットワークを介してホスト計算機と接続するホストインターフェース部と、
ディスク装置と接続するディスクインターフェース部と、
ストレージ装置の制御情報を格納し、キャッシュメモリとして機能するメモリ部と、
ストレージ装置を制御するプロセッサ部と、
前記ホストインターフェース部、前記ディスクインターフェース部、前記メモリ部及び前記プロセッサ部を相互に接続する相互結合部と、
前記ホスト計算機によって読み書きされるデータを暗号化する暗号化機能部と、
を備え、
前記プロセッサ部は、
前記ホスト計算機からデータの更新要求があった場合は、
前記更新要求に係る更新前のデータと更新データとの差分データを、当該差分データに対応する暗号鍵を用いて暗号化し、
前記暗号化されたデータを、所定の領域に書き込み、
前記ホスト計算機からデータの再現要求があった場合は、
前記再現要求に係る差分データを取得し、
前記取得された差分データを復号化し、
前記復号化された差分データを用いて再現要求に係るデータを再現し、

前記再現されたデータを、前記差分データに対応する暗号鍵とは異なる暗号鍵を用いて暗号化し、

前記暗号化されたデータを、前記差分データが格納されていた領域とは異なる領域に書き込むことを特徴とするストレージ装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、記憶装置、特にデータを１つ又は複数のディスク装置に格納するディスクアレイ制御装置、複数のディスクアレイ制御装置やテープライブラリ制御装置、光ディスクライブライ制御装置、半導体ディスク制御装置などのソリッドステートディスク装置、フラッシュメモリに代表される不揮発メモリを利用したストレージ装置などから構成されるストレージ装置に関する。

【背景技術】

【０００２】

企業や官公庁において、個人情報を記録したデジタルデータが増加している。さらに、情報流出に対する企業への法規制も始まっている。そのため、個人情報を初めとするデジタルデータの管理の安全性や流出の危険への対応が急務となっている。

【０００３】

現在、一般的な技術として、アプライアンス型装置をストレージ制御装置と共に利用し、ストレージ装置内のデータを暗号化する方法がある（非特許文献１、特許文献２、参照。）。

【０００４】

この方法でデータを暗号化することによって、ストレージ装置内のデータが暗号化される。これによって、ストレージ装置自体や搭載する磁気記憶装置（ＨＤＤ）が盗難にあったとしても、不正入手した者はデータを解読することが困難となる。

【０００５】

また、ストレージ装置において、異なる論理ボリューム間でのデータの共有化機能であるボリュームミラー機能やスナップショット機能が知られている（非特許文献２及び３参照。）。

【０００６】

また、ストレージ装置内においての書き込み時の動作に関して、キャッシュメモリとディスク装置との書き込み動作に、ライトアフターと呼ばれる方式がある。具体的には、上位ＣＰＵと接続される複数のホストアダプタと、アレイディスクと接続される複数のディスクアダプタと、これらのアダプタに共用される一時記憶用キャッシュメモリとは、これらアダプタ及びキャッシュメモリに共用されるコモンバス上に挿抜自在に取り付けられる。規模を拡大するには、必要な数だけこれらアダプタ及びキャッシュメモリを付加するだけでよい。アダプタキャッシュメモリ及びコモンバスは二重化され、障害時の縮退運転を可能とし、また各アダプタ及びキャッシュメモリとコモンバスとの結合部は、活線挿抜可能としシステム無停止で保守点検部品交換を可能とする記憶システムが知られている（特許文献１参照）。

【非特許文献１】“Securing Networked Storage whitepaper”、ＤＥＣＲＵ　Ｉｎｃ．、２００４年

【非特許文献２】“Data Protection with Storage Networks PartII”、ｐ．２５－４５、［online］、２００４年、ＳＮＩＡ、インターネット＜URL：http://www.snia.org/education/tutorials/fall2004/backup/data_protection_partII.pdf＞

【非特許文献３】“Examination of Disk-based Data Protection Technologies”、ｐ．２３－３６、［online］、２００５年、ＳＮＩＡ、インターネット＜URL：http://www.snia.org/education/tutorials/spr2005/data-management/ExaminationofDiskBasedDataProtection-v5.pdf＞

【特許文献１】特開平７－２０９９４号公報

【特許文献２】米国特許公開公報第２００４／０１５３６４２号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、ユーザが求める高度で機密性の高い暗号化と従来からユーザの利用するデータ複製機能、それぞれの機能の整合性を保ちつつ、それによるホストコンピュータに対する少ない性能劣化という要求が従来技術においては全く考慮されていない。
【０００８】
前述のような暗号化アプライアンス装置を備えるシステムにおいて、暗号鍵の情報がシステムの管理運用方法などの人的要因によって盗み出された場合はデータが解読されてしまう。
【０００９】
また、ストレージ制御装置とアプライアンス型の暗号化装置とを用い、ストレージ装置で、データの複製機能やスナップショット取得機能を利用した場合は、複数のデータが同一の暗号鍵を持って暗号化される。従って、鍵を不正に入手した者に対して、複数のデータの解読を許す脆弱性の増大を招く。
【００１０】
この問題点にについて、図２２に示す模式図を用いて説明する。
【００１１】
図２２において、ホストコンピュータ１０４、ストレージ装置１０１、暗号化アプライアンス２０１がネットワーク１０５を介して接続している。
【００１２】
暗号化アプライアンス２０１は、ストレージ装置１０１の上位階層に位置する。ホスト１０４がストレージ装置１０１に対してデータの書き込みを要求したデータは、暗号化アプライアンス２０１によって暗号化され、暗号化されたデータが記憶装置１０１に書き込まれる。また、ホスト１０４が読み出し要求したデータは暗号化アプライアンス２０１によって復号化されてホスト１０４に送られる。
【００１３】
また、ストレージ装置１０１において、データ複製手段２０４によって、ホスト１０４がアクセスする論理ボリュームＬＶＯＬ１　２０２と、論理ボリュームＬＶＯＬ２　２０３とで複製関係を構成する。この場合は、同一の暗号鍵「鍵１」を用いて暗号化されたデータが、二つの論理ボリュームに複製される。
【００１４】
ここで、ストレージ装置１０１において、データ複製の一機能であるｓｎａｐｓｈｏｔを実行する。ここでは、ｍｉｒｒｏｒ－ｓｐｒｉｔ方式でｓｎａｐｓｈｏｔを実行する。この場合、論理ボリュームＬＶＯＬ１　２０２と論理ボリュームＬＶＯＬ２　２０３とはミラーリングの関係が解除される。この後、論理ボリュームＬＶＯＬ１　２０２への書き込まれたデータはＬＶＯＬ２　２０３には反映されない。
【００１５】
この場合、暗号化アプライアンス２０１は、ストレージ装置１０１内部のデータ複製の動作を知ることはできないので、論理ボリュームＬＶＯＬ１　２０２への新たな書き込みデータも全て同一の暗号鍵を用いて暗号化する。この結果、同一の鍵を用いた暗号化データが倍増する。この後、さらに、ｓｎａｐｓｈｏｔ処理を繰り返せば、同一の暗号鍵を使用する論理ボリュームがさらに増加する。
【００１６】
本発明はこのような問題点に鑑みてされたものであり、データの暗号化とデータ複製機能とを連携して、無用なデータ保護の脆弱性を取り除くことによって安全で高信頼でかつ機密性を高めたストレージ装置を顧客に提供することを目的とする。
【課題を解決するための手段】
【００１７】

本発明は、ネットワークを介してホスト計算機と接続するホストインターフェース部と、ディスク装置と接続するディスクインターフェース部と、ストレージ装置の制御情報を格納し、キャッシュメモリとして機能するメモリ部と、ストレージ装置を制御するプロセッサ部と、前記ホストインターフェース部、前記ディスクインターフェース部、前記メモリ部及び前記プロセッサ部を相互に接続する相互結合部と、前記ホスト計算機によって読み書きされるデータを暗号化する暗号化機能部と、を備え、前記ディスク装置には第１の論理ボリューム及び第２の論理ボリュームが設定されており、前記第１の論理ボリュームと前記第２の論理ボリュームとでコピーペアが設定されており、前記プロセッサ部は、前記第１の論理ボリュームに格納されているデータを読み出し、前記読み出されたデータを、当該第１の論理ボリュームに対応する暗号鍵を用いて復号化し、前記復号化されたデータを、前記第２の論理ボリュームに対応する暗号鍵を用いて暗号化し、前記暗号化されたデータを前記第２の論理ボリュームに書き込むことによって、前記第１の論理ボリュームの内容を前記第２の論理ボリュームに複製し、前記ホスト計算機から前記第１の論理ボリュームへのデータの書き込み要求があった場合は、当該書き込みデータを前記第１の論理ボリュームに対応する暗号鍵を用いて暗号化し、暗号化されたデータを前記第１の論理ボリューム及び第２の論理ボリュームに書き込み、前記コピーペアの状態が変化した場合は、前記第１の論理ボリュームに対応する暗号鍵を変更し、当該変更した暗号鍵を用いて前記書き込みデータを暗号化し、暗号化されたデータを前記第１の論理ボリュームに書き込むことを特徴とする。

【発明の効果】

【００１８】

本発明によると、より安全で機密性の高い暗号化データの管理と、ストレージ装置が提供する特徴的な機能であるデータ複製機能との効率的な連携が実現される。

【発明を実施するための最良の形態】

【００１９】

以下に、本発明の実施の形態を、図面を参照して説明する。

（第１の実施形態）

図１は、本発明の第１の実施の形態の計算機システムの構成ブロック図である。

【００２０】

複数のホスト１０４（１０４Ａ、１０４Ｂ、１０４Ｃ）がネットワーク１０５を介してストレージ装置１０１に接続されている。ストレージ装置１０１には、ディスク装置群１０３が接続されている。また、ネットワーク１０５にもディスク装置群１０３が接続されている。また、管理端末１０７がネットワーク１０６を介してストレージ装置１０１に接続されている。

【００２１】

ホスト１０４は、ネットワーク１０５を介してストレージ装置１０１に要求を送信し、その結果を受信する。ストレージ装置１０１は、ホスト１０４からの要求に従って、ディスク装置群１０２又は１０３のデータを読み書きする。

【００２２】

ストレージ装置１０１は、ホストインターフェース部１１１、ディスクインターフェース部１１３、ＭＰ（プロセッサ）部１１３、メモリ部１１４、管理部１１５、及び、これらを相互に結合する相互結合部１１６を備える。またディスクインターフェース部１１３は暗号化機能部１１７を備える。

【００２３】

ホストインターフェース部１１１は、ネットワークを介して送信された要求を受信して、その要求の結果を送信元に送信する。

【００２４】

ディスクインターフェース部１１３は、ディスク装置群１０２に接続され、ディスク装置群１０２のデータを読み書きする。またディスク装置群１０２の構成を設定する。

【００２５】

ＭＰ部１１２は、ストレージ装置１０１内部で規定された処理を実行する。また、ホストインターフェース部１１１が受信した要求を解析して、その要求に基づいた処理を実行する。

【００２６】

メモリ部１１４は、データを一時的に記憶する。また、ディスク装置群１０２に書き込むためのデータを一時的に格納するキャッシュメモリとして機能する。また、ストレージ装置１０１の各部で共有する情報を格納するための共有メモリとして機能する。

【００２７】

管理部１１５は、ＭＰ部１１２と互いに接続しており、ストレージ装置１０１を管理する。

【００２８】

本実施の形態では、ホストインターフェース部１１１、ディスクインターフェース部１１３、及び、メモリ部１１４、は二重化されており、ストレージ装置１０１は、それぞれを二つずつ備えている。また、ＭＰ部１１２は、ホストインターフェース部１１１及びディスクインターフェース部１１３それぞれに備えられる。なお、本発明のストレージ装置１０１は、この構成に限られず、ホストインターフェース部１１１、ディスクインターフェース部１１３、及び、メモリ部１１４は、それぞれ一又は複数個備えられていてもよい。

【００２９】

ディスク装置群１０２及び１０３は、一又は複数の磁気ディスク装置を備える。本実施の形態では、ディスク装置群１０８は１６個の磁気ディスク装置を備えている。ストレージ装置１０１のディスクインターフェース部１１３Ａがそのうちの８個の磁気ディスク装置をアクセスし、ディスクインターフェース部１１３Ｂが残りの８個をアクセスするように設定されている。

【００３０】

また、ディスク装置群１０３は、ネットワークに直接接続されている。ホスト１０４は、このディスク装置群１０３にネットワーク１０５を介して直接アクセスしたり、ストレージ装置１０１を介してアクセスすることができる。このディスク装置群１０３は、例えば、ディスクアレイ装置であったり、仮想ディスク装置である。

【００３１】

なお、本実施の形態のディスク装置群１０２及び１０３は、磁気ディスク装置を備えるが、これに限られず、別の記憶装置、例えば、テープライブラリや光ディスクライブラリ、半導体ディスク装置、フラッシュメモリアレイ、ＤＶＤライブラリ等の記憶媒体を備えていてもよい。

【００３２】

管理端末１０７は、ネットワーク１０６を介してストレージ装置１０１の管理部１１５に接続されている。管理端末１０７は、ストレージ装置１０１の管理部１０７と通信をして、ストレージ装置１０１の各種設定等を管理する。

【００３３】

図２は、ホストインターフェース部１１１及びＭＰ部１１２の詳細な構成のブロック図である。

【００３４】

ホストインターフェース部１１１は、ホストインターフェース制御部３１１、制御部３１２及びメモリ３１７を備えている。制御部３１２は、内部バス／ＳＷ機能部３１３、ＤＭＡ機能部３１４及び相互結合部インターフェース制御部３１５を備える。

【００３５】

ホストインターフェース制御部３１１は、一又は複数のネットワーク１０５との接続経路を有し、ネットワーク１０５を介してデータを送受信する。

【００３６】

内部バス／ＳＷ機能部３１３は、ホストインターフェース部１１１の各部を相互に接続

するバスの機能と、各部に相互に送受信されるデータを転送するスイッチの機能とを備えている。

【００３７】

ＤＭＡ機能部３１４は、データを相互結合部１１６を介して送受信させる機能を備える。相互結合網インターフェース制御部３１５は、相互結合部１１６との接続経路を有し、相互結合部１１６を介してデータを送受信する。

【００３８】

メモリ３１７は、ホストインターフェース部１１６によって送受信されるデータのキャッシュメモリとして機能する。

【００３９】

ＭＰ部１１２は、ＭＰ（プロセッサ）３２１、ネットワークインターフェース３２２、メモリ３２３、ブリッジ３２４を備えている。

【００４０】

ＭＰ（プロセッサ）３２１は、ＭＰ部１１２の処理の主体となるプロセッサである。

【００４１】

ネットワークインターフェース３２２は、管理部１１５との接続経路を有し、管理部１１５とでデータを送受信する。

【００４２】

メモリ３２３は、ＭＰ３２１によって実行されるプログラムや各種情報等が格納される。

【００４３】

ブリッジ３２４は、ホストインターフェース部１１１の内部バス／ＳＷ機能部３１３との接続経路を有し、ホストインターフェース部１１１とでデータを送受信する。なお、内部バス／ＳＷ機能部３１３とブリッジ３２４とは、直接接続されていなくてもよい。例えば、ブリッジと相互結合部１１６との接続経路を接続し、相互結合部１１６を介してホストインターフェースと通信可能に接続してもよいし、他の接続方法でもよい。

【００４４】

図３は、ディスクインターフェース部１１３及びＭＰ部１１２の詳細な構成のブロック図である。

【００４５】

ディスクインターフェース部１１３の構成は、前述したホストインターフェース部１１１と同様である。すなわち、ディスクインターフェース部１１１は、ディスクインターフェース制御部３１９、制御部３１２及びメモリ３１７を備えている。制御部３１２は、内部バス／ＳＷ機能部３１３、ＤＭＡ機能部３１４及び相互結合部インターフェース制御部３１５を備える。

【００４６】

そしてさらに、ＲＡＩＤ機能部３１６と暗号化エンジン３１８とを備える。

【００４７】

ディスクインターフェース制御部は、一又は複数のディスク装置群１０２との接続パスを有し、ディスク装置群１０２とでデータを送受信する。

【００４８】

ＲＡＩＤ機能部３１６は、ディスク装置群１０２に備えられる各磁気ディスク装置のＲＡＩＤ機能を実現する。このＲＡＩＤ機能によって、ディスク装置群１０２に論理ボリュームが設定される。

【００４９】

暗号化エンジン３１８は、ディスクインターフェース部１１３を通過するデータを、暗号化鍵を用いて暗号化する。暗号化エンジン３１８による暗号化処理及び暗号化鍵の管理はＭＰ部１１２によって実行される。すなわち、暗号化エンジン３１８の機能がＭＰ部１１２によって処理されることによって、暗号化機能部１１７が構成されている。

【００５０】

図４は、メモリ部１１４の詳細な構成のブロック図である。

【００５１】

メモリ部１１４は、メモリ４１１及び制御部４１６を備える。

【００５２】

制御部４１６は、メモリコントローラ４１２、内部バス／ＳＷ機能４１３、ＤＭＡ機能４１４及び相互結合網インターフェース制御部４１５を備える。

【００５３】

メモリ４１１は、例えばＲＡＭであり、データを一時的に格納する。

【００５４】

内部バス／ＳＷ機能４１３、ＤＭＡ機能４１４及び相互結合網インターフェース制御部４１５は、前述したホストインターフェース部１１１又はディスクインターフェース部１１３と同様の機能を備える。

【００５５】

メモリコントローラ４１２は、メモリ４１１のデータの読み書きを制御する。

【００５６】

次に、本実施の形態のデータの暗号化方法について説明する。

【００５７】

図５は、ホスト１０４がストレージ装置１０１にデータを書き込む場合の処理を模式的に示す説明図である。

【００５８】

ストレージ装置１０１において、論理ボリューム００及び０１が構成されている。論理ボリュームとは、ホスト１０４から一つのディスク装置として認識できる論理的な領域である。この論理ボリュームは、管理端末１０７からの指示等によってあらかじめ設定しておく。

【００５９】

なお、論理ボリューム００の実際の物理的な格納位置は、ディスク装置群１０２の複数の磁気ディスク装置５０４Ａ～Ｈに設定されている。また、論理ボリューム０１の実際の物理的な格納位置は、ディスク装置群１０２の複数の磁気ディスク装置５０５Ａ～Ｈに設定されている。従って、ディスクインターフェース部１１３Ａが磁気ディスク装置５０４をアクセスし、ディスクインターフェース部１１３Ｂは磁気ディスク装置５０５をアクセスする。

【００６０】

また、論理ボリューム００と論理ボリューム０１とは、論理ボリューム００を主ボリュームとするミラーリング機能を実現するボリュームペア５０３が設定されている。すなわち、論理ボリューム００に書き込まれたデータは、論理ボリューム００にも書き込まれる。この結果、論理ボリューム００の内容と論理ボリューム０１の内容とは常に一致した状態が保たれる。

【００６１】

以下に、ホスト１０４がストレージ装置１０１に構成されている論理ボリューム００に書き込みデータ「ＤＴ０」を書き込む場合の動作を説明する。

【００６２】

ホスト１０４から論理ボリューム００への書き込み要求があった場合は、ホストインターフェース部１１１Ａがこの要求を受け付ける。ホストインターフェース部１１１Ａは、書き込みデータＤＴ０をメモリ部１１４Ａに格納する。メモリ部１１４Ａには、各論理ボリュームに対応するキャッシュメモリ領域が設定されている。そして、ホストインターフェース部１１４Ａは、メモリ部１１４Ａのキャッシュメモリ領域にデータＤＴ０を書き込んだ旨をメモリ部１１４に設定されている共有メモリ部に格納する。

【００６３】

ディスクインターフェース部１１３Ａ及び１１３Ｂは、この共有メモリの内容を取得して、書き込みデータがメモリ部１１４Ａに格納されたことを検出する。そして、メモリ部

１１４Ａに格納された書き込みデータＤＴ０を、ディスク装置群１０２の書き込み要求に係る領域に格納する。

【００６４】

このとき、ディスクインターフェース部１１３Ａは、書き込み要求に係るディスク装置群１０２の領域、すなわち、論理ボリューム００に関して、ボリューム管理テーブルを参照して暗号鍵を取得する。ボリューム管理テーブルは、図８に説明するように、どの論理ボリュームはどの暗号鍵を用いて暗号化をするかが格納されている。

【００６５】

ディスクインターフェース部１１３Ａは、暗号鍵を取得すると、暗号化機能部１１７Ａにおいて当該暗号鍵を用いて、書き込みデータを暗号化する。そして、暗号化したデータをディスク装置群１０２の書き込み要求に係る領域に格納する。

【００６６】

また、ディスクインターフェース部１１３Ｂも同様に、書き込み要求に係るディスク装置群１０２の領域、すなわち、論理ボリューム０１に関して、ボリューム管理テーブルを参照して暗号鍵を取得する。そして、暗号化機能部１１７Ｂにおいて、取得した暗号鍵を用いて書き込みデータＤＴ０を暗号化し、暗号化したデータをディスク装置群１０２に格納する。

【００６７】

図６は、ストレージ装置１０１におけるデータ書き込みの処理のフローチャートである。

【００６８】

図５において前述したように、ストレージ装置１０１において、ホストインターフェース部１１１Ａは、書き込みデータＤＴ０をメモリ部１１４Ａのキャッシュメモリ領域に格納する。そして、その旨をメモリ部１１４の共有メモリ領域に格納する。これによって、書き込み要求に係る論理ボリューム００へのデータの書き込みが処理される。また、当該論理ボリューム００とミラーリングペアに設定されている論理ボリューム０１へのデータの複製が処理される（Ｓ６０１）。

【００６９】

ディスクインターフェース部１１３Ａは、共有メモリ領域に格納された情報に基づいて、データを書き込むためのライトタスクを生成する（Ｓ６０２）。

【００７０】

このライトタスクによって、ディスクインターフェース部１１３Ａにおいて次の処理が実行される。

【００７１】

まず、書き込み要求に係る論理ボリューム００を元にボリューム管理テーブルを参照する。そして、当該論理ボリューム００は暗号化をするか否かを取得する。そして、暗号化する場合には当該論理ボリュームに対応する暗号鍵を取得する。そして、暗号化機能部１１７Ａにおいて、取得した暗号鍵を用いて書き込みデータを暗号化する（Ｓ６０３）。

【００７２】

そして、暗号化された書き込みデータを、書き込み要求に係る領域に書き込んで、ライトタスクを終了する（Ｓ６０４）。

【００７３】

同様に、ディスクインターフェース部１１３Ｂは、共有メモリ領域に格納された情報に基づいて、データを書き込むためのライトタスクを生成する（Ｓ６０５）。

【００７４】

そして、このライトタスクによって、書き込み要求に係る論理ボリューム０１に対応する暗号鍵を取得して、書き込みデータを暗号化する（Ｓ６０６）。そして、暗号化されたデータを書き込み要求に係る領域に書き込んで、ライトタスクを終了する（Ｓ６０７）。

【００７５】

この図６のフローチャートによって、ホスト１０４の書き込み要求が処理される。そし

て、必要な場合は、書き込みデータを暗号化する。

【００７６】

なお、この図６の処理は、実際にはホストインターフェース部１１１又はディスクインターフェース部１１３に備えられたＭＰ部１１２によって実行される。以降も同様に、ホストインターフェース部１１１又はディスクインターフェース部１１３の処理として記載するが、実際にはＭＰ部１１２によって実行される処理である。なお、ＭＰ部１１２Ａ乃至１１２Ｄのうち、何れのＭＰ部１１２が処理の主体となってもよい。

【００７７】

次に、論理ボリュームのボリュームペアの設定を説明する。

【００７８】

ボリュームペアの設定にはさまざまな方法が考えられる。ボリュームペア状態の生成に関連して、元々別の論理ボリュームである二つの論理ボリュームを、正側の論理ボリューム及び副側の論理ボリュームとしてボリュームペアを生成するための初期設定が必要となる。より具体的には、正側の論理ボリュームに存在するデータを、副側の論理ボリュームにコピーして二つの論理ボリュームを同期させる。この処理を初期コピー処理と呼ぶ。

【００７９】

以降は、前述の図６のフローチャートの処理によって、正側と副側の論理ボリュームにデータが書き込まれる。

【００８０】

なお、正側の論理ボリュームのデータは当該論理ボリュームに対応する暗号鍵によって暗号化されている、一方、副側の論理ボリュームにも対応する暗号鍵が設定されている。

【００８１】

そこで、正側の論理ボリュームのデータを読み出して、暗号化されているデータを復号化し、さらに副側の論理ボリュームに対応する暗号鍵によって当該データを暗号化した後、副側の論理ボリュームに保存する処理（初期コピー処理）を実行する。

【００８２】

図７は、ストレージ装置１０１におけるデータ複製初期実行処理のフローチャートである。

【００８３】

まず、ディスクインターフェース部１１３Ａは、正側に設定された論理ボリュームのデータを読み出し、メモリ部１１４の作業領域、すなわちキャッシュメモリ領域に格納する（Ｓ６０８）。このとき、読み出したデータを、当該論理ボリュームに対応する暗号鍵によって復号化して、復号化したデータをキャッシュメモリに格納する（Ｓ６０９）。

【００８４】

次に、ディスクインターフェース部１１３Ｂは、メモリ部１１４に格納されているデータを、副側に設定された論理ボリュームにデステージする（Ｓ６１０）。このとき、ディスクインターフェース部１１４Ｂは、当該論理ボリュームに対応する暗号鍵を取得して、当該データを暗号化する（Ｓ６１１）。そして、暗号化されたデータを、副側に設定された論理ボリュームに対応するディスク装置群１０２の領域に格納する（Ｓ６１２）。

【００８５】

この図７の処理によって、正側に設定された論理ボリュームの内容が、副側に設定された論理ボリュームに格納される。このとき、ディスクインターフェース部１１３は、ボリューム管理テーブルを参照して、当該論理ボリュームに対応する暗号鍵を取得して、正側に設定された論理ボリュームに対応する暗号鍵を用いて復号化し、副側に設定された論理ボリュームに対応する暗号鍵を用いて暗号化する。

【００８６】

図８は、ボリューム管理テーブルの説明図である。

【００８７】

ボリューム管理テーブルは、前述のように、どの論理ボリュームがどの暗号鍵を用いるかを示すテーブルである。

【００８８】
このテーブルはあらかじめ管理者等によって設定されて、ストレージ装置１０１のメモリ部１１４に格納されている。なお、このボリューム管理テーブルは、暗号化機能部１１７によってアクセスが可能であればどのような場所にあってもよい。例えば、ディスクインターフェース部１１３のメモリ３１７に置かれていてもよいし、他の場所でもよい。
【００８９】
ボリューム管理テーブルは、ボリューム暗号化可否テーブル７１０及び暗号鍵テーブル７２０を備えている。
【００９０】
ボリューム暗号化可否テーブル７１０は、番号７１１、論理ボリュームＩＤ７０１、暗号化可否フィールド７０２及び所有者ＩＤ７０３を備えている。
【００９１】
番号７１１は、各エントリ毎に付される識別子である。論理ボリュームＩＤ７０１は、論理ボリューム名を示す識別子である。暗号化可否フィールド７０２はその論理ボリュームを暗号化するか否かを示す識別子である。暗号化フィールド７０２が「１」に設定されている場合は、その論理ボリュームは暗号化することを示し、「０」に設定されている場合はその論理ボリュームは暗号化しない。所有者ＩＤ７０３は、その論理ボリュームをアクセスする所有者を示す識別子である。所有者は、例えば、ホスト１０４の識別子やホスト１０４のユーザの識別子である。
【００９２】
暗号鍵テーブル７２０は、番号７０５、論理ボリュームＩＤ７０６及び暗号鍵７０４を備えている。
【００９３】
番号７０５は、各エントリ毎に付される識別子である。論理ボリュームＩＤ７０６は、論理ボリューム名を示す識別子である。暗号鍵７０４は、その論理ボリュームに対応する暗号鍵である。
【００９４】
暗号化機能部１１７は、このボリューム管理テーブルを参照して、論理ボリュームを暗号化するか否かを判断する。そして、暗号化する場合は、その論理ボリュームに対応する暗号鍵を、暗号鍵７０４からパラメタとして取得する。そして、取得した暗号鍵を用いて、その論理ボリュームに格納するデータを暗合化する。
【００９５】
このように、本発明の第１の実施の形態の計算機システムでは、ホストからの書き込みデータを論理ボリュームに書き込むときに、その論理ボリュームに対応する暗号鍵を用いて書き込みデータを暗号化して、データを書き込む。このようにすることによって、論理ボリューム毎に異なる暗号鍵を用いて異なる暗号かデータが格納されるので、ストレージ装置１０１のデータの安全性が高まる。
（第２の実施形態）
次に本発明の第２の実施の形態について説明する。
【００９６】
前述の第１の実施の形態では、ディスクインターフェース部１１３が暗号化機能部１１７を備えていた。これに対して本実施の形態では、その他の部（ホストインターフェース部１１１又はメモリ部１１４）が暗号化機能部１１７を備える。なお、第１の実施の形態と同一の構成には同一の符号を付し、その説明は省略する。
【００９７】
図９は、第２の実施の形態の計算機システムにおいて、ホスト１０４がストレージ装置１０１にデータを書き込む場合の処理を模式的に示す説明図である。
【００９８】
ストレージ装置１０１において、論理ボリューム００及び０１が構成されている。この論理ボリュームは、管理端末１０７からの指示等によってあらかじめ設定しておく。

【００９９】
なお、論理ボリューム００の実際の物理的な格納位置は、ディスク装置群１０２の磁気ディスク装置５０４に設定されている。また、論理ボリューム０１の実際の物理的な格納位置は、ディスク装置群１０２の磁気ディスク装置５０５に設定されている。従って、ディスクインターフェース部１１３Ａが磁気ディスク装置５０４をアクセスし、ディスクインターフェース部１１３Ｂは磁気ディスク装置５０４をアクセスする。
【０１００】
また、論理ボリューム００と論理ボリューム０１とは、論理ボリューム００を主ボリュームとするミラーリング機能を実現するボリュームペアが設定されている。
【０１０１】
以下に、ホスト１０４がストレージ装置１０１に構成されている論理ボリューム００に書き込みデータ「ＤＴ０」を書き込む場合の動作を説明する。
【０１０２】
ホスト１０４から論理ボリューム００への書き込み要求があった場合は、ホストインターフェース部１１３Ａがこれを受け付ける。
【０１０３】
そして、ホストインターフェース部１１１Ａは、書き込み要求に係る論理ボリューム００に関して、ボリューム管理テーブルを参照して暗号鍵を取得する。ホストインターフェース部１１１Ａは、暗号鍵を取得すると、暗号化機能部１１７Ａにおいて当該暗号鍵を用いて書き込みデータを暗号化する。そして、暗号化したデータをメモリ部１１４Ａの当該書き込み要求に対応する領域に書き込みデータＤＴ０を格納する。このとき、ホストインターフェース部１１１Ａは、メモリ部１１４ＡにデータＤＴ０を格納した旨をメモリ部１１４Ａ又は１１４Ｂに設定されている共有メモリ部に格納する。
【０１０４】
ここで、ディスクインターフェース部１１３Ａは、この共有メモリの内容を取得して、暗号化された書き込みデータがメモリ部１１４Ａに格納されたことを検出する。そして、ディスクインターフェース部１１３Ａは、キャッシュメモリ領域に格納されたデータをディスク装置群１０２の書き込み要求に係る領域に格納する。このデータは、書き込み要求に係る論理ボリューム００に対応した暗号鍵を用いて暗号化されている。
【０１０５】
一方、副側の論理ボリューム０１への書き込み処理は、次のような手順で実行される。
【０１０６】
まず、ホストインターフェース部１１１Ｂが、共有メモリの内容を取得して、暗号化された書き込みデータがメモリ部１１４Ａに格納されたことを検出する。そして、この暗号化データに関して、ボリューム管理テーブルを参照して、書き込み要求に係る論理ボリューム００に対応する暗号鍵を取得する。そして、暗号化機能部１１７Ｂにおいて、取得した暗号鍵を用いてデータを復号化する。次に、ホストインターフェース部１１１Ｂは、ボリューム管理テーブルを参照して、副側に設定されている論理ボリューム０１に対応する暗号鍵を取得して、復号化したデータを、取得した暗号鍵を用いて暗号化する。そして、暗号化されたデータをメモリ部１１４Ｂのキャッシュメモリ領域に格納する。この旨は共有メモリに格納される。
【０１０７】
ディスクインターフェース部１１３Ｂは、この共有メモリの内容を取得して、暗号化された書き込みデータがメモリ部１１４Ｂに格納されたことを検出する。そして、ディスクインターフェース部１１３Ｂは、キャッシュメモリ領域に格納されたデータをディスク装置群１０２の書き込み要求に係る領域に格納する。このデータは、書き込み要求に係る論理ボリューム０１に対応した暗号鍵を用いて暗号化されている。
【０１０８】
図１０は、本実施の形態のストレージ装置１０１におけるデータ書き込みの処理のフローチャートである。

【０１０９】
図９において前述したように、ストレージ装置１０１において、ホストインターフェース部１１１Ａは、まず、書き込みデータＤＴ０を、書き込み要求に係る論理ボリュームに対応する暗号鍵を、ボリューム管理テーブルを参照して、取得する。そして、取得した暗号鍵を用いて当該データを暗号化する（Ｓ９０１）。
【０１１０】
次に、ホストインターフェース部１１１Ａは、暗号化したデータをメモリ部１１４Ａのキャッシュメモリ領域に格納する（Ｓ９０２）。そして、その旨をメモリ部１１４の共有メモリ領域に格納する。これによって、書き込み要求に係る論理ボリューム００へのデータの書き込みが処理される。
【０１１１】
一方、ホストインターフェース部１１１Ｂは、この共有メモリの内容を取得して、暗号化された書き込みデータがメモリ部１１４Ｂに格納されたことを検出すると、データ複製処理を実行する（Ｓ９０３）。
【０１１２】
まず、ホストインターフェース部１１１Ｂは、キャッシュメモリ領域に格納された暗号化データをホストインターフェース部１１１Ｂのメモリ３１７に設定されているバッファ領域に読み込む（Ｓ９０４）。
【０１１３】
次に、ホストインターフェース部１１１Ｂは、ボリューム管理テーブルを参照して、書き込み要求に係る論理ボリューム００に対応する暗号鍵を取得する。そして、暗号化機能部１１７Ｂにおいて、取得した暗号鍵を用いてデータを復号化する（Ｓ９０５）。
【０１１４】
次に、ホストインターフェース部１１１Ｂは、ボリューム管理テーブルを参照して、副側に設定されている論理ボリューム０１に対応する暗号鍵を取得する。そして、復号化したデータを取得した暗号鍵を用いて暗号化する（Ｓ９０６）。そして、暗号化されたデータをメモリ部１１４Ｂのキャッシュメモリ領域に格納する（Ｓ９０７）。そして、その旨をメモリ部１１４の共有メモリ領域に格納する。これによって、書き込み要求に係る論理ボリューム０１へのデータの書き込みが処理される。
【０１１５】
この図１０のフローチャートによって、ホスト１０４の書き込み要求が処理される。そして、必要な場合は、書き込みデータを暗号化する。
【０１１６】
このように、暗号化機能部１１７は、ストレージ装置１０１のホストインターフェース部１１１が備えることができる。ホストインターフェース部１１１が暗号化機能部１１７を備えることによって、ホスト１０４から送信されたデータを直ちに暗号化でき、相互結合部１１６を何度もデータが行き来することがなくなりストレージ装置１０１内部の負荷が低減できる。また、外部に接続されたディスク装置群１０３に暗号化データを格納する場合は、外部のディスク装置群１０３と直接通信するホストインターフェース部１１１によってデータを暗号化／復号化することができ、ストレージ装置１０１内部の負荷が低減できる。
【０１１７】
次に、第２の実施の形態の変形例として、メモリ部１１４が暗号化機能部１１７を備えた場合の例を説明する。
【０１１８】
図１１は、第２の実施の形態の変形例の計算機システムにおいて、ホスト１０４がストレージ装置１０１にデータを書き込む場合の処理を模式的に示す説明図である。
【０１１９】
前述したように、ホスト１０４からの書き込み要求は、ホストインターフェース部１１１Ａが処理して、書き込みデータをメモリ部１１４Ａのキャッシュメモリ領域に格納する

。この際に、暗号化機能部１１７Ａにおいて、論理ボリュームに対応する暗号鍵を用いてデータを暗号化する。

【０１２０】

より具体的には、ホストインターフェース部１１１が、書き込みデータをキャッシュメモリ領域に格納する際に、ボリューム管理テーブルを参照して、書き込み要求に係る論理ボリューム００に対応する暗号鍵を取得する。そして、暗号化機能部１１７Ａにおいて、取得した暗号鍵を用いて書き込みデータを暗号化する。暗号化されたデータは、その後、前述のようにディスクインターフェース部１１３Ａによって、ディスク装置群１０２の当該領域に書き込まれる。

【０１２１】

一方、ディスクインターフェース部１１３Ｂは、キャッシュメモリ領域に格納された暗号化データに関して、ボリューム管理テーブルを参照して、書き込み要求に係る論理ボリューム００に対応する暗号鍵を取得する。そして、暗号化機能部１１７Ｂにおいて、取得した暗号鍵を用いてデータを復号化して、復号化したデータをメモリ部１１４Ｂのキャッシュメモリ領域に格納する。そして、ディスクインターフェース部１１３Ｂは、ボリューム管理テーブルを参照して、副側に設定されている論理ボリューム０１に対応する暗号鍵を取得して、復号化したデータを、取得した暗号鍵を用いて暗号化してメモリ部１１４Ｂのキャッシュメモリ領域に格納する。そして、ディスクインターフェース部１１３Ｂは、キャッシュメモリ領域に格納されたデータをディスク装置群１０２の書き込み要求に係る領域に格納する。

【０１２２】

なお、暗号化機能部１１７の機能を制御するＭＰ部１１２は、ホストインターフェース部１１１に備えられているＭＰ部１１２でもよいし、ディスクインターフェース部１１３に備えられているＭＰ部１１２であってもよい。

【０１２３】

図１２は、本実施の形態のメモリ部１１４の構成のブロック図である。

【０１２４】

メモリ部１１４の構成は前述した図４の構成と同様であるが、暗号化エンジン４１７を備える点が第１の実施の形態と異なる。すなわち、暗号化エンジン４１８の機能が何れかのＭＰ部１１２によって処理されることによって、暗号化機能部１１７が構成されている。

【０１２５】

このように、暗号化機能部１１７は、ストレージ装置１０１のメモリ部１１４が備えることができる。メモリ部１１４が暗号化機能部を備えることによって、相互結合部１１６の帯域を使用することなくデータの暗号化／復号化をキャッシュメモリ領域内での処理とすることができる。

【０１２６】

第３の実施の形態では、前述した第１又は第２の実施の形態の計算機システムにおいて、論理ボリューム間のコピーペアの処理に関する。なお、第１の実施の形態と同一の構成には同一の符号を付し、その説明は省略する。

【０１２７】

図１３は、第３の実施の形態の計算機システムにおいて、ホスト１０４がストレージ装置１０１にデータを書き込む場合の処理を模式的に示す説明図である。

【０１２８】

本実施の形態のストレージ装置１０１は、前述の第２の実施の形態と同様に、ホストインターフェース部１１１が暗号化機能部１１７を備えている。なお、暗号化機能部１１７は、ディスクインターフェース部１１３が備えていても、メモリ部１１４が備えていてもよい。

【０１２９】

また、本実施の形態では、ストレージ装置１０１において、三つの論理ボリュームが構

成されている。

【０１３０】

論理ボリューム００の実際の物理的な格納位置は、ディスク装置群１０２の磁気ディスク装置５０４に設定されている。また、論理ボリューム０１の実際の物理的な格納位置は、ディスク装置群１０２の磁気ディスク装置５０５に設定されている。また、論理ボリューム０２の物理的な格納位置は、ストレージ装置１０１の外部に接続されているディスク装置群１０３の磁気ディスク装置５０６に設定されている。従って、ディスクインターフェース部１１３Ａが論理ボリューム００をアクセスし、ディスクインターフェース部１１３Ｂは論理ボリューム０１をアクセスする。また、論理ボリューム０２は、ホストインターフェース部１１１Ｂによってアクセスされる。

【０１３１】

さらに、これらの論理ボリュームは、ミラーリング機能によってコピーペア状態が設定されている。具体的には、論理ボリューム００と論理ボリューム０１とがコピーペア状態に設定されている。また、論理ボリューム００と論理ボリューム０２とがコピーペア状態に設定されている。

【０１３２】

ここで、前述の第１又は第２の実施の形態では、コピーペア状態となっているお互いの論理ボリューム毎に暗号鍵を変えた。これに対して、本実施の形態では、コピーペアが同期状態である場合（Ｓｙｎｃ、ＰＡＩＲ、又は、Ｍｉｒｒｏｒ　Ａｃｖｉｖｅとも呼ぶ）は、ペアに設定されている論理ボリュームでは同一の暗号鍵を用いる。これは、コピーペアが同期状態である場合は、各論理ボリュームに同一のデータを格納しているため、セキュリティ状の観点から同一の暗号鍵で問題ないという考えである。

【０１３３】

そして、同期状態のコピーペアが解消状態になった場合（ＰＡＩＲ　ＤＥＬＥＴＥ又はＳＩＭＰＬＥＸと呼ぶ）又は、コピーペアが一時停止状態となった場合（Ｍｉｒｒｏｒ　Ｓｐｌｉｔ又はＭｉｒｒｏｒ　Ｂｒａｋｅと呼ぶ）には、それ以降に受信した書き込み要求データについて、暗号鍵を変更して暗号化する。

【０１３４】

以下に、本実施の形態の動作を説明する。

【０１３５】

ホスト１０４から論理ボリューム００への書き込み要求があった場合は、ストレージ装置１０１において、前述の第２の実施の形態と同様に、書き込み要求に係る論理ボリューム００に対応する暗号鍵によってデータを暗号化して、論理ボリューム００にデータを格納する。

【０１３６】

このとき、論理ボリューム００とコピーペア状態となっている論理ボリューム０１に対しても、同一の暗号鍵Ｋｅｙ０を用いて暗号化したデータを格納する。同様に、論理ボリューム０２に対しても、同一の暗号鍵Ｋｅｙ０を用いて暗号化したデータを格納する。

【０１３７】

ここで、ストレージ装置１０１にＭｉｒｒｏｒ－Ｓｐｒｉｔ命令が発効され、論理ボリューム００と論理ボリューム０１とで設定されているコピーペアが一時停止状態（１１０４）に設定された場合を説明する。

【０１３８】

ストレージ装置１０１は、コピーペアが一時停止状態（１１０４）となったことを検出した場合は、主側の論理ボリューム００の暗号鍵を変更する。副側の論理ボリューム０１では、コピーペアは同期していないので、以前の暗号鍵Ｋｅｙ０によって暗号化されたデータが格納された状態である。

【０１３９】

なお、論理ボリューム０２は引き続き論理ボリューム００とペア同期状態であるので、主側の論理ボリューム００と同時に暗号鍵を変更する。

【０１４０】
その後、論理ボリューム００への書き込み要求があった場合は、変更された新たな暗号鍵Ｋｅｙ１によって書き込みデータが暗号化され、論理ボリュームに格納される。同様に、論理ボリューム０２にも暗号鍵Ｋｅｙ１によって暗号化されたデータが格納される。
【０１４１】
図１４は、本実施の形態のストレージ装置１０１におけるデータ書き込みの処理のフローチャートである。なお、ここでは二つの論理ボリュームが既にコピーペアが設定されており、同期状態である。
【０１４２】
まず、コピーペアの状態が同期状態から変化があるか否かを検出する。ステップ１２０１において、コピーペアがＤＥＬＥＴＥすなわち解消されたか否かを判定する。そして、ステップ１２０２において、コピーペアがＳＵＳＰＥＮＤすなわち一時停止状態であるか否かを判定する。
【０１４３】
コピーペア状態に変化があると判定した場合は、コピーペア状態変化フラグをセットして、ステップ１２０５に移行する。
【０１４４】
コピーペア状態に変化がない場合はステップ１２０３に移行し、ボリューム管理テーブルを参照して、書き込み要求に係る論理ボリュームに対応する暗号鍵を用いてデータを暗号化する。そして、メモリ部１１４のキャッシュメモリ領域に暗号化データを格納する（Ｓ１２０４）。
【０１４５】
ステップＳ１２０５では、異なる暗号鍵を生成する。そして生成した暗号鍵を、当該論理ボリュームに対応する暗号鍵に設定する。そして、生成した暗号鍵と当該論理ボリュームＩＤとを、ボリューム管理テーブルに登録する（Ｓ１２０６）。このとき、新暗号鍵登録フラグをセットし、コピーペア状態変化フラグをリセットする。これによって、書き込み処理の度に暗号鍵の更新処理をすることを防ぐ。
【０１４６】
このステップ１２０６の処理と同時に、新たに設定した暗号鍵を用いて書き込みデータを暗号化する（Ｓ１２０７）。
【０１４７】
そして、メモリ部１１４のキャッシュメモリ領域に暗号化データを格納する（Ｓ１２０４）。
【０１４８】
ステップ１２０４を実行した後、正側の論理ボリュームへのライトタスクを生成し（Ｓ１２０８）、副側の論理ボリュームへのライトタスクを生成する（Ｓ１２１２）。
【０１４９】
その後、暗号鍵の変更処理がすれ違ったか否かを判定する（Ｓ１２０９）。この処理は、例えば磁気ディスク装置の故障の発生によって、コピーペア状態が突然変化した場合に備えて、暗号化データをキャッシュメモリ領域からディスク装置群１０２に転送する処理の前に、暗号鍵が変更されていないかを再度確認する。すれ違いに判定には、新暗号鍵登録フラグの有無を確認することによって行う。
【０１５０】
暗号鍵の変更がなく、すれ違いがないと判定した場合は、暗号化データをディスク装置群１０２に格納する処理をそのまま実行して終了する。
【０１５１】
一方、もし鍵の変更があり、すれ違いがあると判定した場合は、再度ボリューム管理テーブルを参照して、暗号鍵を取得し、取得した暗号鍵でデータを暗号化する。このとき、必要であればデータを復号化してから暗号化する（Ｓ１２１０）。
【０１５２】

そして、改めて正側の論理ボリュームへのライトタスクを生成して（Ｓ１２１１）、処理を終了する。

【０１５３】

このようにすることによって、コピーペア状態の変更があった以後の書き込みデータは状態変化前とは異なる暗号鍵を用いて暗号化される。もちろん、鍵の変更処理ステップＳ１２０５は状態変化検出のはじめの１回だけ行われる。最初のステップＳ１２１２は副ボリュームへのライト処理として、コピー状態が一時中断の場合に、将来再度コピー状態が同期したときに、コピーすべきデータライト処理として差分情報管理される。一般的にはＲｅｓｙｎｃとか呼ばれる処理である。

【０１５４】

図１５は、本実施の形態のボリューム管理テーブルの説明図である。

【０１５５】

図７において前述した第１の実施の形態のボリューム管理テーブルと同様だが、暗号鍵テーブル７２０に、さらに、エリアＩＤ１３０５を備える。

【０１５６】

エリアＩＤ１３０５は、暗号鍵の情報を細分化する。“エリア”によって指定された範囲や大きさは適当な大きさを選べばよい。エリアＩＤ１３０５は、例えばＬＢＡ（Ｌｏｇｉｃａｌ　Ｂｌｏｃｋ　Ａｄｄｒｅｓｓ）を用いる。これによって、論理ボリューム内の特定の領域に対応した暗号鍵を設定できる。

【０１５７】

また、暗号鍵テーブル７２０は、一つの論理ボリュームに対して複数持つ。前述のように、コピーペアの状態の変化によって、論理ボリュームに対応する暗号鍵が変更される。変更された暗号鍵は、暗号鍵テーブル７２０の履歴として保存する。例えば、コピーペア状態が同期から中断状態となった場合は、暗号鍵が更新され、以前の暗号鍵は暗号鍵テーブルの履歴に保存される。また、コピーペアが中断状態から最同期状態に変更する場合は、この履歴を検索して、更新前の暗号鍵を取得する。

【０１５８】

なお、前述した第１乃至第３の実施形態による処理はそれぞれ単独で利用しても構わないし、組み合わせて利用しても構わない。例えば、第１の実施形態と、第３の実施の形態のコピー機能とを組み合わせてもよい。この場合、例えば、図１５に示すボリューム管理テーブルを使用することで鍵管理情報が増加し、その容量が、あらかじめ決めておいておいたある限界値（ｘｘＭＢなど）を超えた場合は、鍵管理方式を第１の実施の形態（図８）に変更する。このようにすることによって、鍵管理情報が際限なく増加することが避けられる。

【０１５９】

また、暗号化機能の実装位置に着目して、複数の種類の部位に暗号化機能部１１７を実装してもよい。すなわち、相互結合部の帯域の利用状況に応じて、ホストインターフェース部１１１、ディスクインターフェース部１１３又はメモリ部１１４にある暗号化機能部１１７を使い分けることができる。

【０１６０】

なお、それ以外にも前述の実施形態における方式をさまざまに組み合わせてもよい。このような方式の切り替えは、例えば、方式切り替えフラグを設定し、同フラグを参照することによって、ＭＰ部１１２は、現在選択されている暗号鍵管理方式に従って処理をする。

（第４の実施形態）

次に、本発明の第４の実施の形態について説明する。

【０１６１】

第４の実施の形態では、前述した第１又は第２の実施の形態の計算機システムにおいて、スナップショット機能における処理に関する。なお、第１乃至第３の実施の形態と同一の構成には同一の符号を付し、その説明は省略する。

【０１６２】
スナップショット機能とは、ホスト１０４からの書き込みがあった場合に、書き込みによって変更となるデータ（差分データ）を格納し、書き込み前の元データには反映しない。そして、所定の操作（Ｓｎａｐｓｈｏｔ命令）があったときに、元データに差分データを反映させて、データを更新する。
【０１６３】
スナップショット機能には、Ｒｅｄｉｒｅｃｔ－ｏｎ－Ｗｒｉｔｅ（ＲｏＷとも称する）方式と、Ｃｏｐｙ－ｏｎ－Ｗｒｉｔｅ（ＣｏＷとも称する）方式との二通りの処理方法がある。
【０１６４】
ここではまずＣｏＷ方式について説明する。
【０１６５】
ＣｏＷ方式とは、Ｓｎａｐｓｈｏｔ命令があったときに、Ｓｎａｐｓｈｏｔ命令以前に書き込まれたデータを、それまでとは異なる新たな待避領域（例えば異なる論理ボリューム）に格納する。Ｓｎａｐｓｈｏｔ命令後の書き込み要求は、そのまま以前の領域に書き込まれる。
【０１６６】
図１６は、第４の実施の形態の計算機システムにおいて、ホスト１０４がストレージ装置１０１にデータを書き込む場合の処理を模式的に示す説明図である。
【０１６７】
本実施の形態のストレージ装置１０１は、前述の第２の実施の形態と同様に、ホストインターフェース部１１１が暗号化機能部１１７を備えている。なお、暗号化機能部１１７は、ディスクインターフェース部１１３が備えていても、メモリ部１１４が備えていてもよい。
【０１６８】
ホスト１０４から書き込み要求があった場合は、ストレージ装置１０１は、前述のように、データを暗号化してメモリ部１１４のキャッシュメモリ領域に格納する。その後ディスクインターフェース部１１３によって、所定の論理ボリュームにデータが格納される。
【０１６９】
ここで、ホスト１０４からＳｎａｐｓｈｏｔ命令が発効された場合の処理について説明する。なお、ここではＲｏＷ方式の処理を説明する。
【０１７０】
ストレージ装置１０１において、ホスト１０４からＳｎａｐｓｈｏｔ命令が発効されたことを検出する。その後、ホスト１０４から書き込み要求を受けると、その書き込み要求に係る論理ボリュームに対応する暗号鍵を変更する。そして、新たな暗号鍵によってデータを暗号化してデータを書き込む。
【０１７１】
このとき、Ｓｎａｐｓｈｏｔ命令以前に格納されたデータＤＴ０は、新たに設定された待避用の領域に移動する。ここでは、外部ディスク装置群１０３に待避用の領域１を設定し、そこにデータを格納する。
【０１７２】
結果として、Ｓｎａｐｓｈｏｔ命令後の書き込みデータは異なる暗号鍵を用いて暗号化され、Ｓｎａｐｓｈｏｔ命令前のデータは待避用の領域に移動される。
【０１７３】
図１７は、本実施の形態のストレージ装置１０１におけるデータ書き込みの処理のフローチャートである。
【０１７４】
ストレージ装置１０１は、Ｓｎａｐｓｈｏｔ命令が発効されたか否かを判定する（Ｓ１５０１）。Ｓｎａｐｓｈｏｔ命令が発行されたと判定した場合は、ステップ１５０４に移行する。Ｓｎａｐｓｈｏｔ命令が発効されていないと判定した場合はステップ１５０２に

移行し、ボリューム管理テーブルを参照して、書き込み要求に係る論理ボリュームに対応する暗号鍵を用いてデータを暗号化する。そして、メモリ部１１４のキャッシュメモリ領域に暗号化データを格納する（Ｓ１５０３）。

【０１７５】

ステップＳ１５０４では、異なる暗号鍵を生成する。そして生成した暗号鍵を、当該論理ボリュームに対応する暗号鍵に設定する。そして、生成した暗号鍵と当該論理ボリュームＩＤとを、ボリューム管理テーブルに登録する（Ｓ１５０５）。このとき、新暗号鍵登録フラグをセットする。そして、新たに設定した暗号鍵を用いて書き込みデータを暗号化する（Ｓ１５０６）。

【０１７６】

そして、メモリ部１１４のキャッシュメモリ領域に暗号化データを格納する（Ｓ１５０３）。

【０１７７】

ステップ１５０３を実行した後、正側の論理ボリュームへのライトタスクを生成する（Ｓ１５０７）。

【０１７８】

その後、暗号鍵の変更処理がすれ違ったか否かを判定する（Ｓ１５０８）。この処理は、例えば磁気ディスク装置の故障の発生によって、コピーペア状態が突然変化した場合に備えて、暗号化データをキャッシュメモリ領域からディスク装置群１０２に転送する処理の前に、暗号鍵が変更されていないかを再度確認する。すれ違いの判定には、新暗号鍵登録フラグの有無の確認によって行う。

【０１７９】

暗号鍵の変更がなく、すれ違いがないと判定した場合は、暗号化データをディスク装置群１０２に格納する処理をそのまま実行して終了する。

【０１８０】

一方、もし鍵の変更があり、すれ違いがあると判定した場合は、再度ボリューム管理テーブルを参照して、暗号鍵を取得し、取得した暗号鍵でデータを暗号化する。このとき、必要であればデータを復号化してから暗号化する（Ｓ１５０９）。

【０１８１】

そして、改めて正側の論理ボリュームへのライトタスクを生成して（Ｓ１５１０）、処理を終了する。

【０１８２】

図１８は、本実施の形態のストレージ装置１０１におけるデータ書き込みの処理の他の例のフローチャートである。

【０１８３】

前述のように、Ｓｎａｐｓｈｏｔ命令後の書き込み要求に対しては、新たな暗号鍵によって暗号化し、Ｓｎａｐｓｈｏｔ以前の旧データと暗号鍵を異ならせる。

【０１８４】

これに対して、Ｓｎａｐｓｈｏｔ命令があったときに、旧データを異なる暗号鍵によって再度暗号化して、待避用の領域に格納し、新たな書き込み要求に対しては暗号鍵を変更しないという手法を用いることができる。

【０１８５】

ストレージ装置１０１は、Ｓｎａｐｓｈｏｔ命令が発効されたと判定した場合に、本フローチャートを実行する。

【０１８６】

まず、正側の論理ボリューム、すなわち、ホスト１０４の書き込み要求に係る論理ボリュームから、Ｓｎａｐｓｈｏｔ命令以前のデータ（旧データ）を取得して、メモリ部１１４のキャッシュメモリ領域に格納する（Ｓ１６０１）。

【０１８７】

次に、ボリューム管理テーブルを参照して、旧データの格納されていた論理ボリューム

に対応する暗号鍵を取得する。そして、暗号化機能部１１７において、取得した暗号鍵を用いて旧データを復号化する（Ｓ１６０２）。

【０１８８】

そして、復号化されたデータを、待避用の領域に格納する処理を実行する（Ｓ１６０３）。まず、ボリューム管理テーブルを参照して、待避用の領域に係る論理ボリュームに対応する暗号鍵を取得する。そして取得した暗号鍵を用いて旧データを暗号化する（Ｓ１６０４）。

【０１８９】

次に、暗号化されたデータを、待避用の領域に係る論理ボリュームに書き込む（Ｓ１６０６）。

【０１９０】

この処理によって、Ｓｎａｐｓｈｏｔ命令前のデータは異なる暗号鍵を用いて暗号化されて待避用の領域に移動される。Ｓｎａｐｓｈｏｔ命令後の書き込みデータはそれまでと同じ暗号鍵を用いて暗号化される。

【０１９１】

このように、本発明の第４の実施の形態では、Ｓｎａｐｓｈｏｔ命令以前の旧データと、Ｓｎａｐｓｈｏｔ命令以降に書き込まれるデータとは、異なる暗号鍵によって暗号化される。

【０１９２】

なお、本実施の形態を前述のＲｏＷ方式に適用することもできる。

【０１９３】

ＲｏＷ方式では、Ｓｎａｐｓｈｏｔ命令があったときに、Ｓｎａｐｓｈｏｔ命令以前に書き込まれたデータ（旧データ）はそのまま元の領域に格納されたままとする。そして、Ｓｎａｐｓｈｏｔ命令後の書き込み要求は、新たな領域（例えば異なる論理ボリューム）に書き込む。

【０１９４】

ＲｏＷは旧データに対する退避コピーを伴わず、新たなデータを旧データと異なる位置に書き込み、元々の論理ボリュームに対するデータ位置管理ポインタのみを新しい位置情報に更新（Ｒｅｄｉｒｅｃｔ）する方式であるので、新規に書き込まれるデータのみに着目して本方式が適用可能である。逆に旧データを、新規の更新ライトにあわせて、異なる暗号鍵で再暗号化して書き戻すという方式もある。

【０１９５】

この場合は図６のＳ６０８～Ｓ６１２の手順において最後のステップで書き込む領域が元の場所と同じであることと等価である。

【０１９６】

次に、本実施の形態の変形例として、ジャーナルを適用したＳｎａｐｓｈｏｔ機能について説明する。

【０１９７】

ここでは、書き込み要求があったときに、旧データに対する更新データを時系列順にジャーナル（ログとも呼ぶ）と呼ばれる領域に格納する。その後、例えばＳｎａｐｓｈｏｔ命令によって、更新データを旧データに反映させることで、Ｓｎａｐｓｈｏｔ時点の旧データが生成される。その後の書き込み要求は、当該データに対する更新データとしてジャーナルに格納される。

【０１９８】

ジャーナルの処理には主に二つの方式がある。

【０１９９】

一つ目は、更新データを反映させた旧データをジャーナルに逐次記録する方式である。これはＢｅｆｏｒｅイメージジャーナルとも呼ばれる。もう一方は、更新データのみをジャーナルに逐次記録していく方式である。これはａｆｔｅｒイメージジャーナルとも呼ばれる。

【０２００】
なお、ジャーナルにデータを格納する動作は、主側ボリュームとは異なる領域（例えば副側のボリューム）をジャーナルとして管理する。従って、前述した第１乃至第３の実施の形態において説明した方式で、暗号鍵を適切に管理する。
【０２０１】
次に、ジャーナルに格納された旧データから、特定の時点のデータを再現する処理を説明する。
【０２０２】
図１９は、ｂｅｆｏｒｅイメージジャーナル方式のデータ再現処理のフローチャートである。
【０２０３】
なお、ｂｅｆｏｒｅイメージジャーナル方式の場合は、更新データはその格納領域に対応する暗号鍵を用いて暗号化されている。
【０２０４】
まず、ディスクインターフェース部１１３は、再現対象の旧データを、ジャーナルから読み出し、メモリ部１１４のキャッシュメモリ領域に格納する（Ｓ１９０１）。なお、メモリ部１１４ではなく、処理の主体となるＭＰ部１１２のメモリ３２３に格納してもよい。
【０２０５】
次に、読み出した旧データを復号化する（Ｓ１９０２）。具体的には、ディスクインターフェース部１１３は、ボリューム管理テーブルを参照して、読み出した旧データに対応する暗号鍵を取得する。そして、暗号化機能部１１７において、取得した暗号鍵を用いて復号化する。
【０２０６】
次に、復号化した旧データを、再現用の領域に書き込む処理を実行する（Ｓ１９０３）。
【０２０７】
まず、ディスクインターフェース部１１３は、ボリューム管理テーブルを参照して、再現用の領域に対応する暗号鍵を取得する（Ｓ１９０４）。なお、再現用の領域は、書き込み要求を受ける主側の論理ボリュームに直接反映してもよい。また、主側の論理ボリュームからコピー（スナップショット）を受ける副側の論理ボリュームでもよい。
【０２０８】
次に、暗号化機能部１１７において、取得した暗号鍵を用いて、旧データを暗号化する（Ｓ１９０５）。
【０２０９】
次に、ディスクインターフェース部１１３は、暗号化したデータを再現用の領域に書き込む（Ｓ１９０６）。
【０２１０】
以上の処理によって、旧データが再現用の領域に再現される。
【０２１１】
なお、図１９の処理は、旧データの読み込み処理（Ｓ１９０１～Ｓ１９０３）と、再現データの書き込み処理（Ｓ１９０４～Ｓ１９０６）とは、それぞれ独立して非同期で実行可能である。従って、再現時点までの複数の旧データ全てについて、まとめて読み出し、復号化した後、データを再現する処理を実行してもよい。
【０２１２】
次に、ａｆｔｅｒイメージジャーナル方式の場合を説明する。
【０２１３】
ａｆｔｅｒイメージジャーナルの場合は、あらかじめ取得した再現したい任意の時点よりも過去のある時点での主側ボリュームのスナップショット（ベースイメージ）である。
【０２１４】

この場合、基本的には図１９の処理と同じである。すなわち再現対象領域（ベースイメージ）の旧データを読み出し（Ｓ１９０１）、復号化し（Ｓ１９０２）、再暗号化して再び書き込む（Ｓ１９０４～１９０６）。

【０２１５】

このジャーナル方式では、ジャーナル、主側のボリューム、再現対象領域（主側のボリュームのｓｎａｐｓｈｏｔや主側ボリュームそのもの）が、それぞれ異なる領域として異なる暗号鍵によって管理する。このようにすることによって、本来の主側のボリューム、ログ、再現ボリュームがそれぞれ適切な暗号鍵で暗号化され、セキュリティが高まる。

（第５の実施の形態）

次に、第５の実施の形態を説明する。

【０２１６】

これまでは、ストレージ装置１０１内での処理を説明した。本実施形態では、ストレージ装置１０１と、外部の記憶装置との連携について説明する。なお、第１の実施の形態と同一の構成には同一の符号を付し、その説明は省略する。

【０２１７】

図２０は、ホスト１０４がディスク装置群１０３にデータにアクセスする処理を模式的に示す説明図である。

【０２１８】

より具体的には、ホスト１０４Ｃが、ネットワーク１０５を介して接続されているディスク装置群１０３に設定されている論理ボリュームに格納されている暗号化データをアクセスする場合の動作である。なお、ディスク装置群１０３には、複製機能によって副側の論理ボリュームが構成されている。

【０２１９】

この場合、ストレージ装置１０１の持つ暗号鍵の情報をホスト１０４Ｃが知る必要がある。そのため、ストレージ装置１０１のメモリ部１１４Ａに暗号鍵管理情報１７２０を格納する。この暗号鍵管理情報１７２０は、図２１に示すボリューム管理テーブルを含んでいる。

【０２２０】

ディスク装置群１０３のデータＤＴ０にアクセスする場合は、ホスト１０４Ｃは、暗号鍵管理情報１７２０を参照して、ＤＴ０の格納されている領域に対応する暗号鍵を取得する。そしてホスト１０４において取得した暗号鍵を用いてデータを暗号化又は復号化する。

【０２２１】

なお、ディスク装置群１０３がストレージ装置１０１同様に暗号化機能を備えている場合は、ホスト１０４Ｃからアクセスがあった場合に、ディスク装置群１０３が、暗号鍵管理情報１７２０を参照して、ＤＴ０の格納されている領域に対応する暗号鍵を取得する。そしてディスク装置群１０３において取得した暗号鍵を用いてデータを暗号化又は復号化して、ホスト１０４Ｃにデータを渡す。

【０２２２】

なお、ストレージ装置１０１は、暗号鍵管理情報１７２０を外部の装置からアクセスさせる又は提供するための通信手段を用意する必要がある。

【０２２３】

そのため、管理端末１０７が、ネットワーク１０６を介してセキュアに暗号鍵管理情報１７２０をアクセスする手段（例えばＳＳＬやＩＰｓｅｃなどの通信路暗号化）を備える。

【０２２４】

また、ストレージ装置１０１と、ホスト１０４又はディスク装置１０３との間で、暗号鍵管理情報１７２０へのアクセス許可のための通信手段を備える。

【０２２５】

ホスト１０４はこれらの手段に対する許可を要求する。許可が得られた場合は、ホスト

１０４は、ストレージ装置１０１に特殊な通信手段を用いてネットワーク１０５を介して暗号鍵管理情報１７２０へのアクセスを要求する。ストレージ装置１０１は、管理部１１５を経由して管理端末１０７によって設定されたホスト１０４に対するアクセス許可情報を参照し、当該ホスト１０４が許可条件を満たしていれば、暗号鍵管理情報１７２０をホスト１０４に転送する。ホスト計算機１０４は、これによって暗号鍵情報を取得して、ディスク装置群１０３上の暗号化データにアクセス可能となる。

【０２２６】

図２１は、本実施の形態の暗号鍵管理情報１７２０に含まれるボリューム管理テーブルの説明図である。

【０２２７】

本実施形態では、図８又は図１５で前述したボリューム管理テーブルに加え、論理ボリュームＩＤ１８０７と、装置ＩＤ１８０８と、実論理ボリュームＩＤ１８０９とを備える。

【０２２８】

論理ボリュームＩＤ１８０７は、ストレージ装置１０１において設定されている識別子である。装置ＩＤは、ディスク装置群１０３に個別に設定される識別子である。実論理ボリュームＩＤ１８０９は、ディスク装置群１０３が用いる内部での論理ボリュームの識別子である。

【０２２９】

このように、第５の実施の形態では、ストレージ装置１０１が、暗号鍵管理情報１７０２へのアクセス手段を備えることによって、外部に接続されたディスク装置群１０３の論理ボリュームのデータの暗号化又は復号化の処理を実行できる。この場合の処理は、前述した第１乃至第４の実施の形態と同一である。

【図面の簡単な説明】

【０２３０】

【図１】本発明の第１の実施の形態の計算機システムの構成ブロック図である。

【図２】本発明の第１の実施の形態のホストインターフェース部及びＭＰ部の詳細な構成のブロック図である。

【図３】本発明の第１の実施の形態のディスクインターフェース部及びＭＰ部の詳細な構成のブロック図である。

【図４】本発明の第１の実施の形態のメモリ部１１４の詳細な構成のブロック図である。

【図５】本発明の第１の実施の形態のデータを書き込む場合の処理を模式的に示す説明図である。

【図６】本発明の第１の実施の形態のデータ書き込みの処理のフローチャートである。

【図７】本発明の第１の実施の形態のデータ複製初期実行処理のフローチャートである。

【図８】本発明の第１の実施の形態のボリューム管理テーブルの説明図である。

【図９】本発明の第２の実施の形態のデータを書き込む場合の処理を模式的に示す説明図である。

【図１０】本発明の第２の実施の形態のデータ書き込みの処理のフローチャートである。

【図１１】本発明の第２の実施の形態の変形例のデータを書き込む場合の処理を模式的に示す説明図である。

【図１２】本発明の第２の実施の形態のメモリ部の構成のブロック図である。

【図１３】本発明の第３の実施の形態のデータを書き込む場合の処理を模式的に示す説明図である。

【図１４】本発明の第３の実施の形態のデータ書き込みの処理のフローチャートである。

【図１５】本発明の第３の実施の形態のボリューム管理テーブルの説明図である。

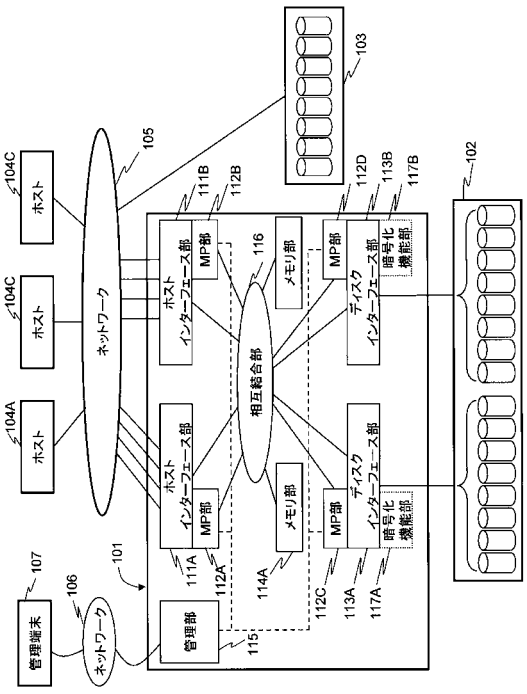
【図１６】本発明の第４の実施の形態のデータを書き込む場合の処理を模式的に示す説明図である。

【図１７】本発明の第４の実施の形態のデータ書き込みの処理のフローチャートである。

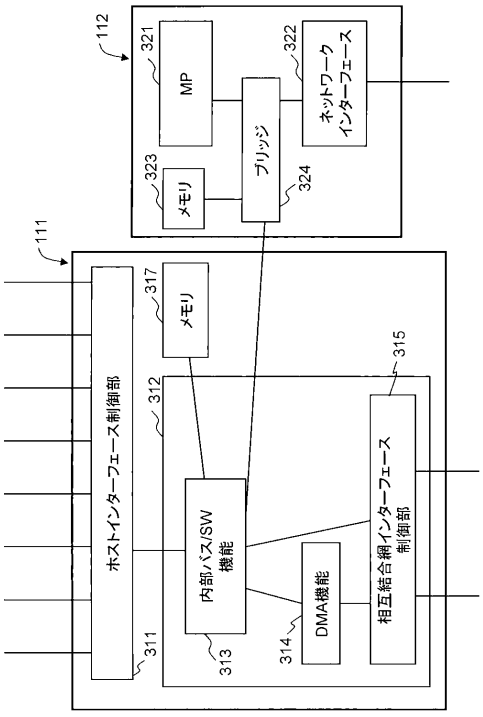
【図１８】本発明の第４の実施の形態のデータ書き込みの処理の他の例のフローチャート

である。
【図１９】本発明の第４の実施の形態のデータ再現処理のフローチャートである。
【図２０】本発明の第５の実施の形態のデータにアクセスする処理を模式的に示す説明図である。
【図２１】本発明の第５の実施の形態のボリューム管理テーブルの説明図である。
【図２２】従来の計算機システムの説明図である。
【符号の説明】
【０２３１】
１０１　　ストレージ装置
１０２　　ディスク装置群
１０３　　ディスク装置群
１０４　　ホスト
１０５　　ネットワーク
１０６　　ネットワーク
１０７　　管理部
１１１　　ホストインターフェース部
１１２　　ＭＰ部
１１３　　ディスクインターフェース部
１１４　　メモリ部
１１５　　管理部
１１６　　相互結合部
１１７　　暗号化機能部
７００　　ボリューム管理テーブル

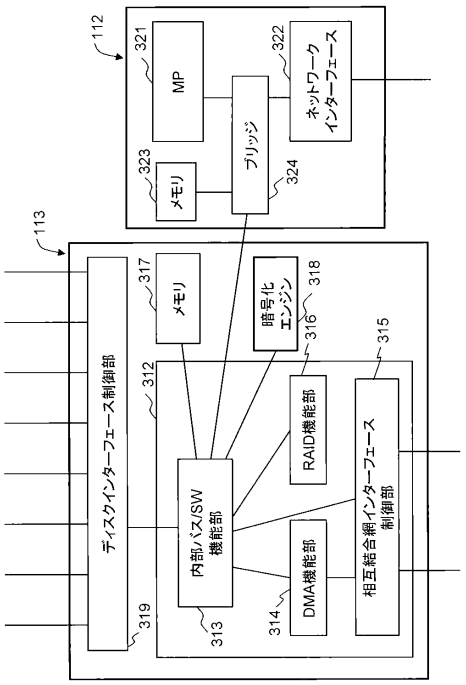
【図１】



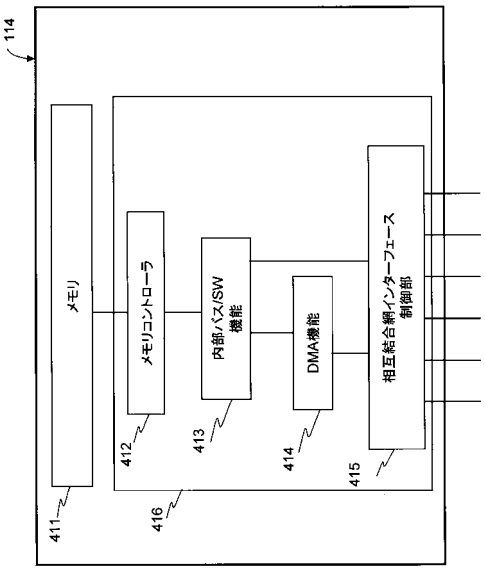
【図２】



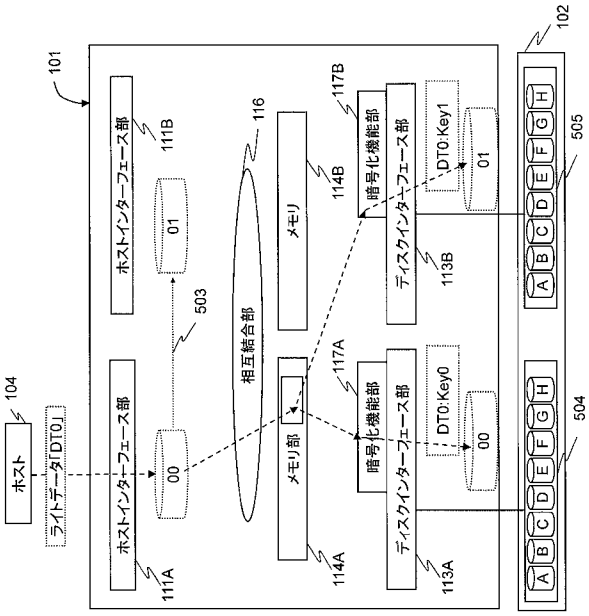
【図３】


112
321
MP
322
ネットワークインターフェース
323
メモリ
プリッジ
324
113
ディスクインターフェース制御部
317
メモリ
暗号化エンジン
318
316
RAID機能部
315
312
内部バス/SW機能部
相互結合網インターフェース制御部
319
313
314
DMA機能部

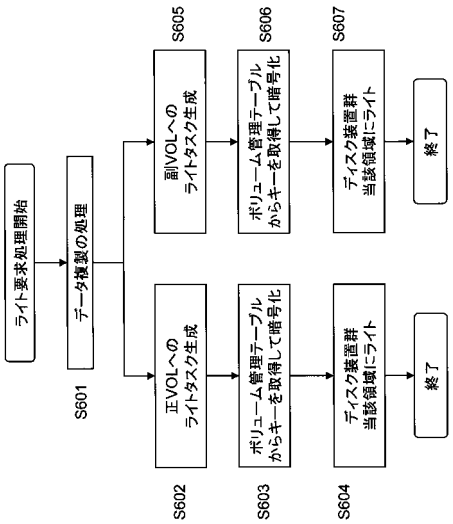
【図４】


114
メモリ
メモリコントローラ
内部バス/SW機能
DMA機能
相互結合網インターフェース制御部
411
412
413
414
415
416

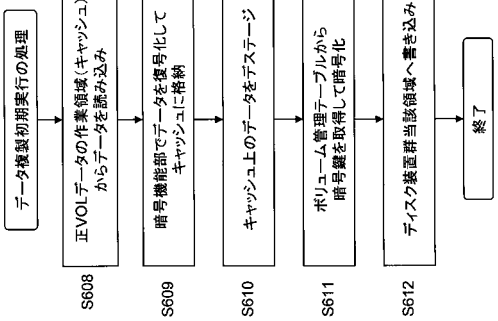
【図５】


101
102
ホスト
104
ライトデータ「DT0」
ホストインターフェース部
111A
111B
00
01
503
相互結合部
116
メモリ部
メモリ
114A
114B
117A
117B
暗号化機能部
ディスクインターフェース部
113A
113B
DT0:Key0
DT0:Key1
A B C D E F G H
504
505

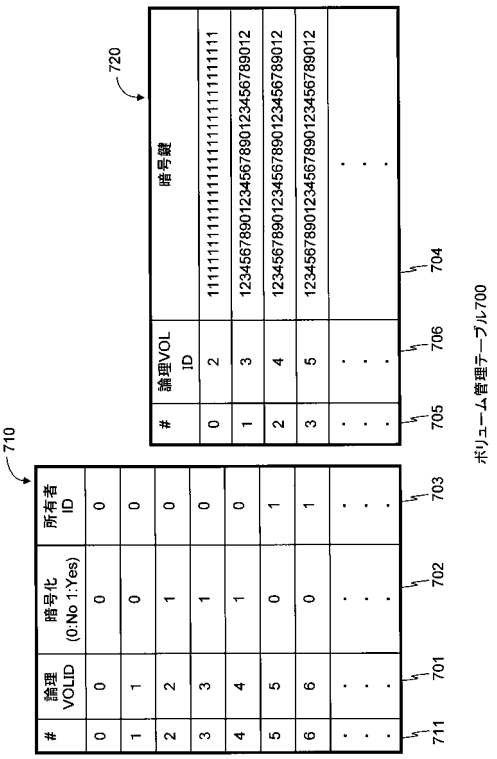
【図６】


ライト要求処理開始
S601
データ複製の処理
正VOLへのライトタスク生成
S602
副VOLへのライトタスク生成
S605
ボリューム管理テーブルからキーを取得して暗号化
S603
ボリューム管理テーブルからキーを取得して暗号化
S606
ディスク装置群当該領域にライト
S604
ディスク装置群当該領域にライト
S607
終了
終了

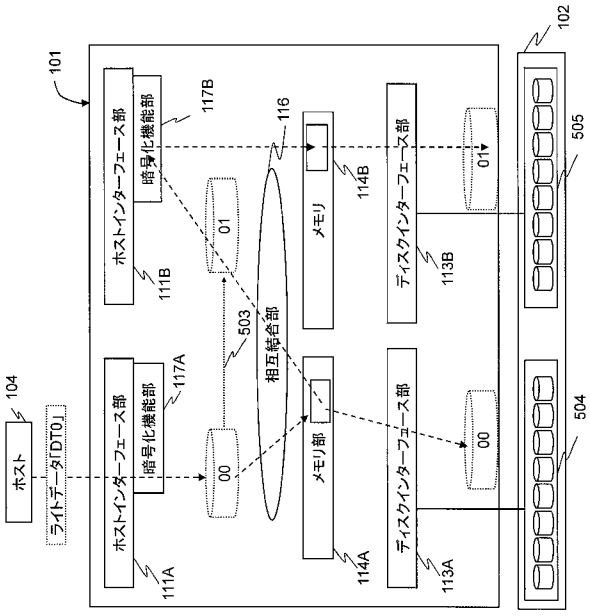
【図７】


データ複製初期実行の処理
正VOLデータの作業領域（キャッシュ）からデータを読み込み
暗号機能部でデータを復号化してキャッシュに格納
キャッシュ上のデータをデスステージ
ボリューム管理テーブルから暗号鍵を取得して暗号化
ディスク装置群当該領域へ書き込み
終了
S608
S609
S610
S611
S612

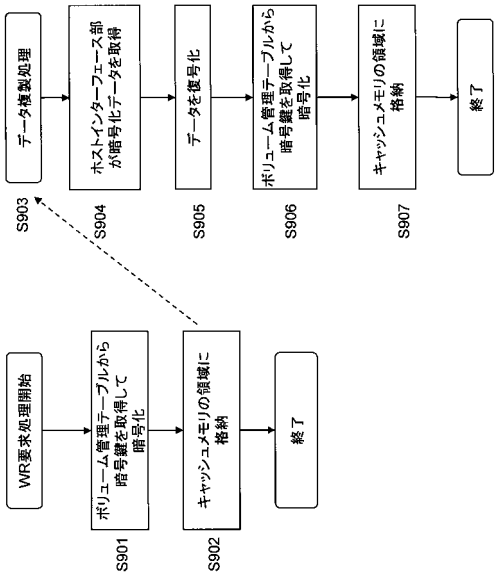
【図８】


710
720
論理VOLID 暗号化(0:No 1:Yes) 所有者ID
論理VOL ID 暗号鍵
ボリューム管理テーブル700
701
702
703
704
705
706
711

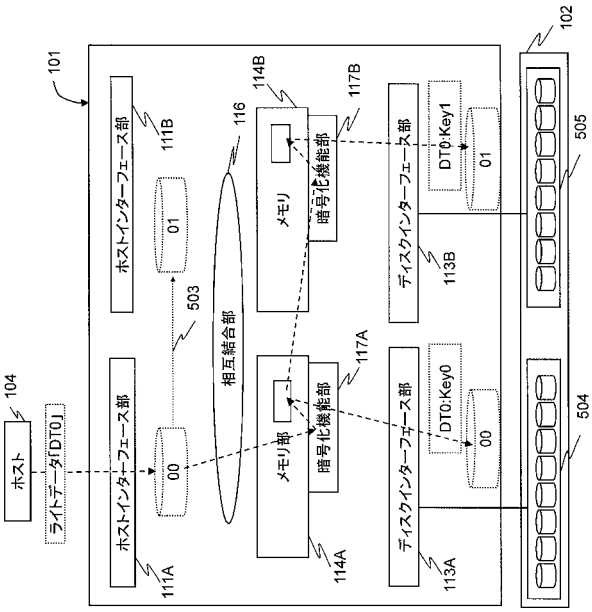
【図９】


ホスト
104
ライトデータ[DTO]
101
ホストインターフェース部
暗号化機能部
111A
117A
00
503
相互結合部
メモリ部
114A
ディスクインターフェース部
113A
504
ホストインターフェース部
暗号化機能部
111B
117B
01
116
メモリ
114B
ディスクインターフェース部
113B
505
102

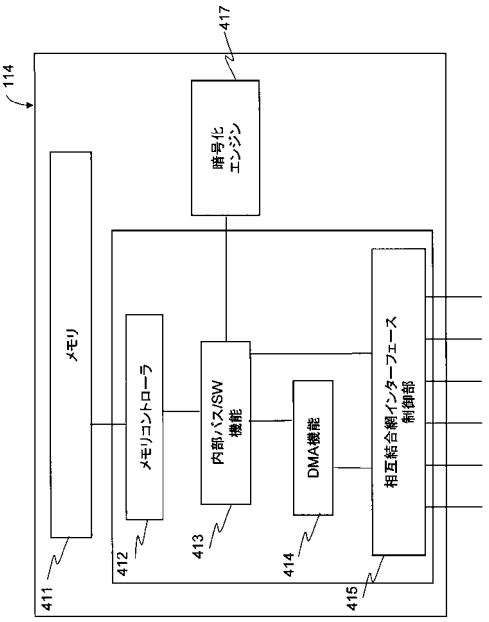
【図１０】


WR要求処理開始
ボリューム管理テーブルから暗号鍵を取得して暗号化
S901
キャッシュメモリの領域に格納
S902
終了
データ複製処理
S903
ホストインターフェース部が暗号化データを取得
S904
データを復号化
S905
ボリューム管理テーブルから暗号鍵を取得して暗号化
S906
キャッシュメモリの領域に格納
S907
終了

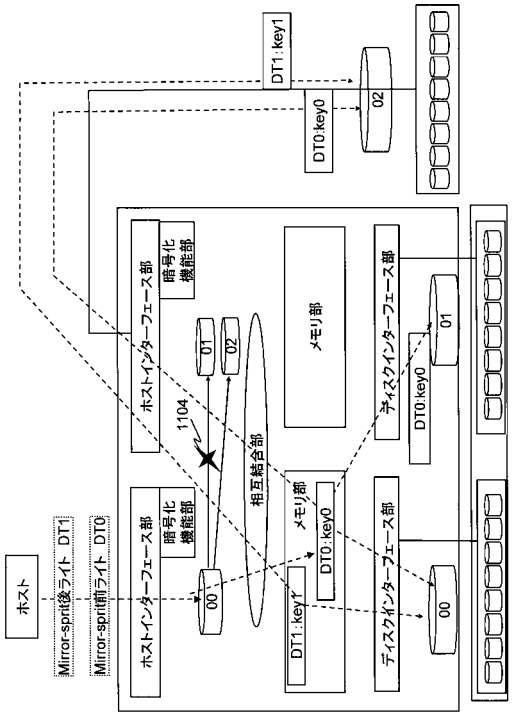
【図１１】



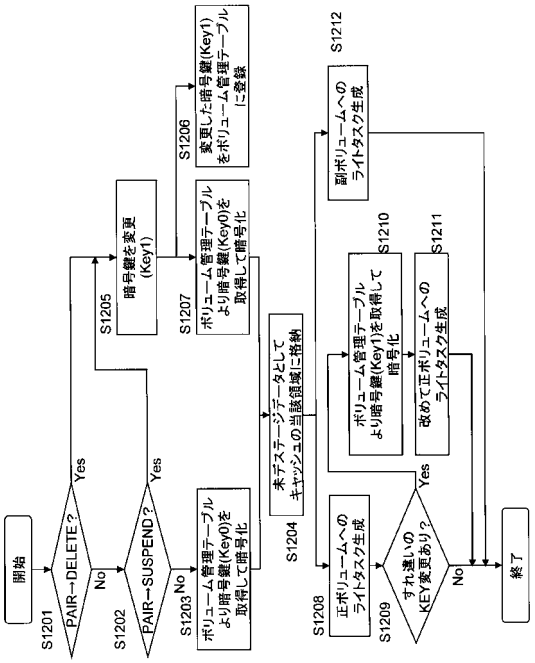
【図１２】



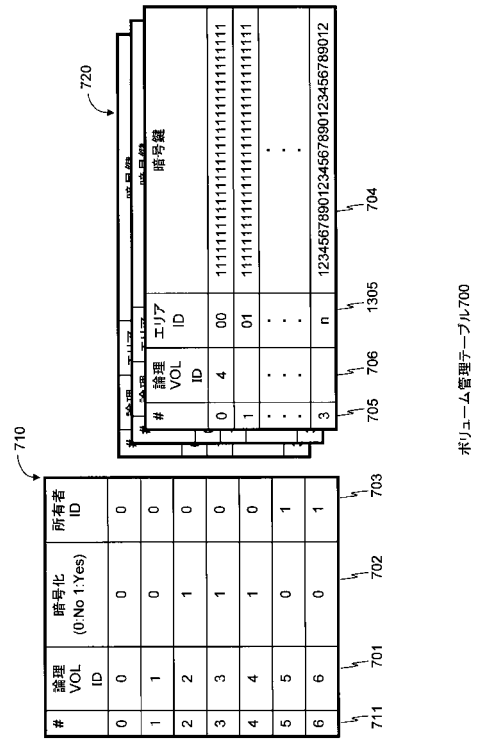
【図１３】



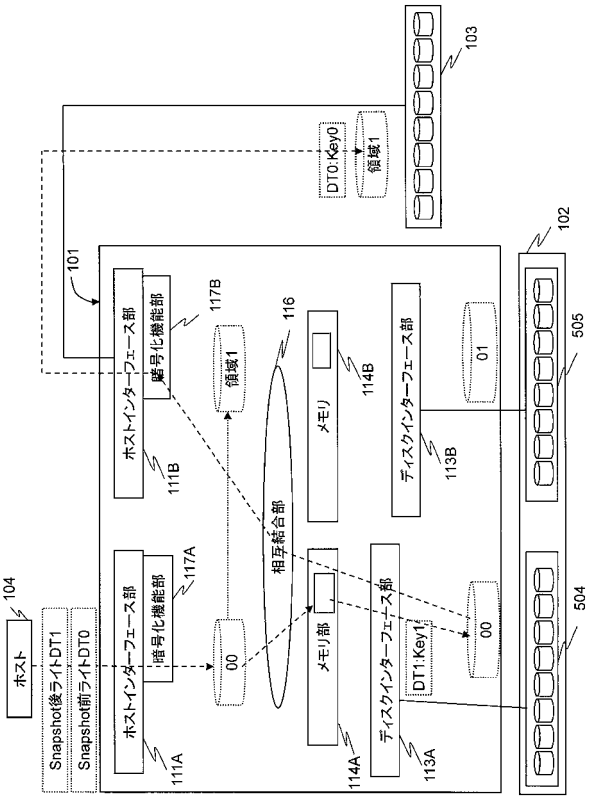
【図１４】



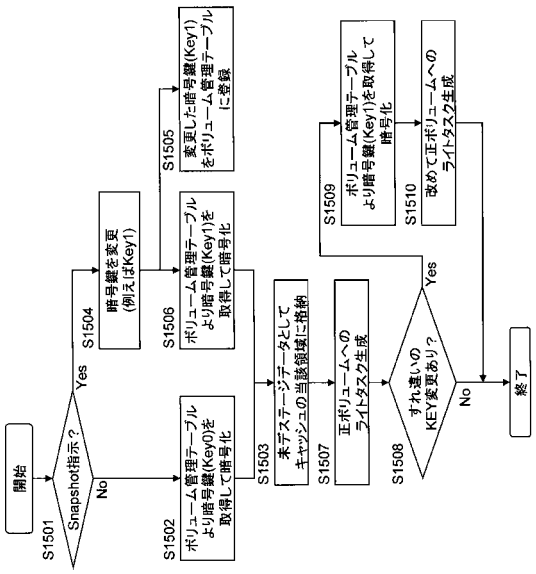
【図１５】



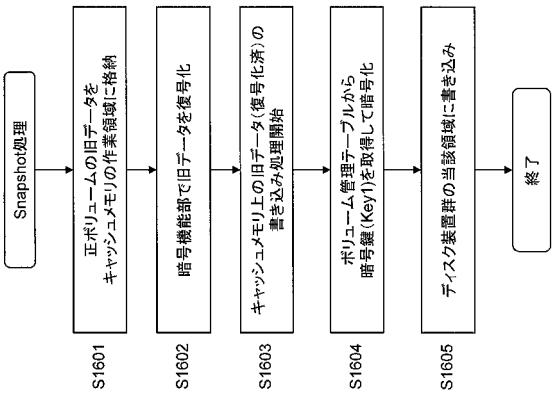
【図１６】



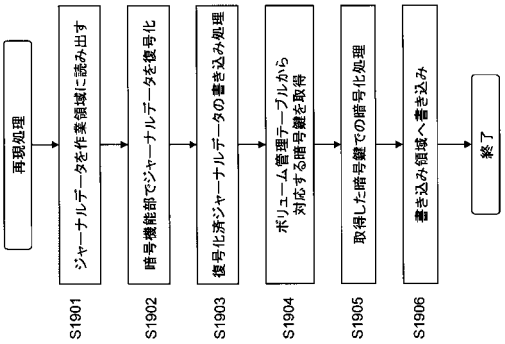
【図１７】



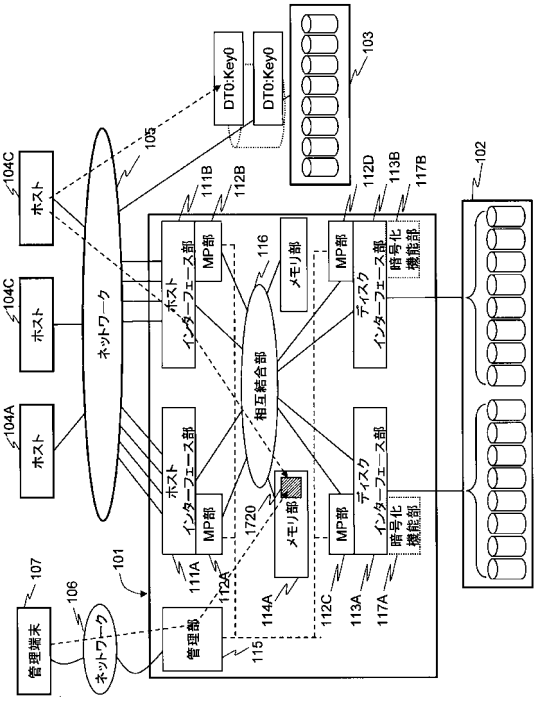
【図１８】



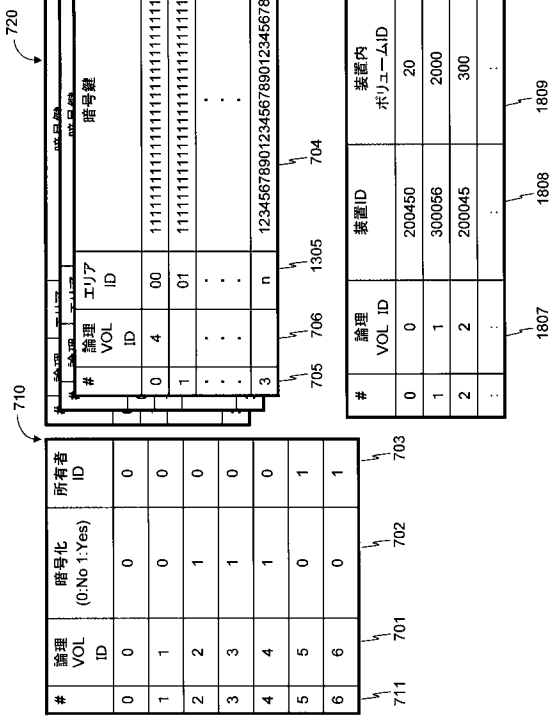
【図１９】



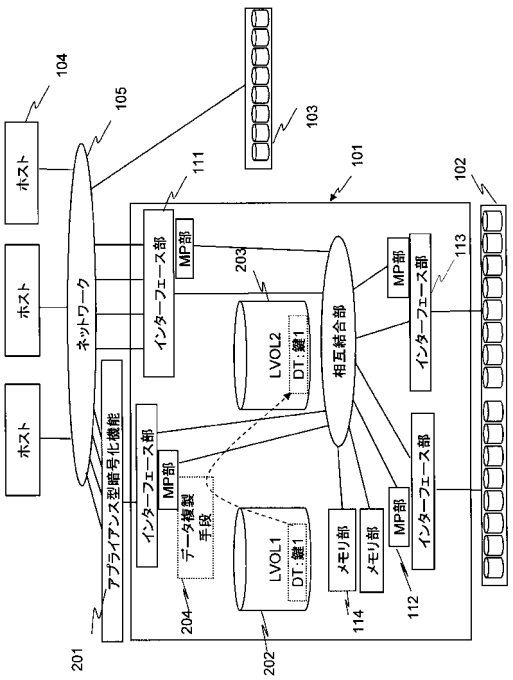
【図２０】



【図２１】



【図２２】



フロントページの続き

(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

審査官　新田　亮

(56)参考文献　特開２００１－３３１３８０（ＪＰ，Ａ）
特開２００５－００４８９３（ＪＰ，Ａ）
特開２００１－３２５２０７（ＪＰ，Ａ）
特開２００４－２９５２７３（ＪＰ，Ａ）
特開２００５－１４９１０１（ＪＰ，Ａ）
特開２００５－０９４７９０（ＪＰ，Ａ）
特開２００５－１３５００３（ＪＰ，Ａ）
特開昭６３－２１１０４５（ＪＰ，Ａ）
米国特許出願公開第２００４／０１５３６４２（ＵＳ，Ａ１）
米国特許出願公開第２００３／００３７２４７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４
Ｇ０６Ｆ　　３／０６
Ｇ１１Ｂ　２０／１０
Ｇ１１Ｂ　２０／１２