(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-362600
(P2004-362600A)
(43)公開日　平成16年12月24日(2004.12.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 13/14	G06F 13/14	310B	5B014
G06F 3/06	G06F 3/06	304H	5B017
G06F 12/14	G06F 12/14	520C	5B065
G06F 13/10	G06F 12/14	530C	
	G06F 13/10	340A	

審査請求 有　請求項の数 2　OL　（全 16 頁）

(21)出願番号　特願2004-212455(P2004-212455)
(22)出願日　平成16年7月21日(2004.7.21)
(62)分割の表示　特願2000-118493(P2000-118493)の分割
原出願日　平成9年5月29日(1997.5.29)

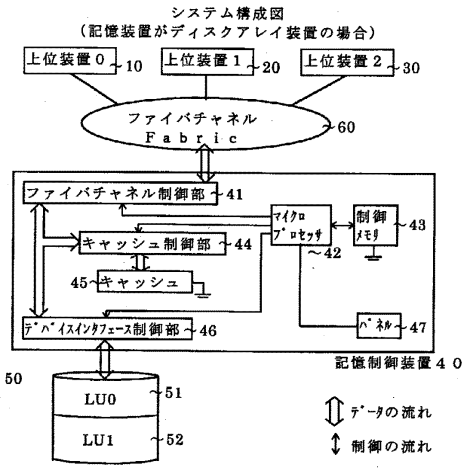
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　眞田　明美
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　中野　俊夫
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内

最終頁に続く

(54)【発明の名称】記憶制御装置及び記憶システム

(57)【要約】
【課題】　上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを防止するセキュリティ機能を設定できる記憶システムを提供する。
【解決手段】　上位装置１０、２０、３０を一意に識別できるN__Ｐｏｒｔ__Ｎａｍｅ情報及び各上位装置がどのＬＵにアクセス可能であるかの情報の入力を、記憶制御装置４０のマイクロプロセッサ４２は受ける事ができる。この情報入力はパネル４７或いは上位装置のユティリティプログラムにより行なう。そして上位装置１０、２０、３０がＬＵにアクセスしてきたときに、このアクセスコマンドに含まれるN__Ｐｏｒｔ__Ｎａｍｅ情報と入力した情報から上位装置を特定し、上位装置がそのＬＵにアクセス可能であるかの情報と比較する。
【選択図】図１

【図１】



【特許請求の範囲】
【請求項１】
ファイバチャネルを介して複数の上位装置と接続される記憶システムにおけるアクセス制御方法であって、
前記記憶システムは、
記憶領域を有し前記上位装置から送信されるデータを記憶する記憶装置と、前記上位装置から前記記憶装置へのアクセスを制御する記憶制御装置を有し、さらに前記記憶制御装置は前記上位装置を識別するＮ＿Ｐｏｒｔ＿Ｎａｍｅと、前記記憶領域を識別するLUN(Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ)と、を有するテーブルを備え、
ＰＬＯＧＩ時に、前記上位装置から前記記憶システムに送信されたＰＬＯＧＩフレームに格納された上位装置の識別情報と前記テーブルに記載されている上位装置の識別情報が一致するか比較し、一致する場合は前記上位装置にログイン可能であることを通知する第一の工程と、
前記ＰＬＯＧＩの承認後の前記上位装置からのＩ/Ｏ要求時に、前記上位装置から前記記憶システムに送信されたＩ/Ｏ要求フレームに格納された上位装置の識別情報及びアクセス要求先の記憶領域の識別情報と前記テーブルに記載されている上位装置の識別情報及びアクセス要求先の記憶領域の識別情報が一致するか比較し、一致する場合は前記上位装置にＩ/Ｏ可能であることを通知する第二の工程とを有し、前記上位装置から前記記憶領域へのアクセスを制御することを特徴とするアクセス制御方法。
【請求項２】
ファイバチャネルを介して複数の上位装置と接続される記憶システムにおけるアクセス制御方法であって、
前記記憶システムは、
記憶領域を有し前記上位装置から送信されるデータを記憶する記憶装置と、前記上位装置から前記記憶装置へのアクセスを制御する記憶制御装置を有し、さらに前記記憶制御装置は前記上位装置を識別するＮ＿Ｐｏｒｔ＿ＩＤと、前記記憶領域を識別するLUN(Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ)と、を有するテーブルを備え、
ＰＬＯＧＩ時に、前記上位装置から前記記憶システムに送信されたＰＬＯＧＩフレームに格納された上位装置の識別情報と前記テーブルに記載されている上位装置の識別情報が一致するか比較し、一致する場合は前記上位装置にログイン可能であることを通知する第一の工程と、
前記ＰＬＯＧＩの承認後の前記上位装置からのＩ/Ｏ要求時に、前記上位装置から前記記憶システムに送信されたＩ/Ｏ要求フレームに格納された上位装置の識別情報及びアクセス要求先の記憶領域の識別情報と前記テーブルに記載されている上位装置の識別情報及びアクセス要求先の記憶領域の識別情報が一致するか比較し、一致する場合は前記上位装置にＩ/Ｏ可能であることを通知する第二の工程とを有し、前記上位装置から前記記憶領域へのアクセスを制御することを特徴とするアクセス制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、上位装置と接続される記憶制御装置、及び記憶制御装置配下の記憶装置から成る記憶システムにおいて、上位装置から記憶制御装置配下の記憶装置へのアクセス要求があった際の、不正アクセス防止手段に関する。
【背景技術】
【０００２】
ネットワーク上の不正アクセス防止に関しては、従来から種々の技術が知られている。
例えば、特開平３－１５２６５２号公報には、ＴＣＰ／ＩＰをサポートするコンピュータシステム間のネットワークセキュリティシステムとして、ログインできるユーザＩＤをメモリに定義しておくことにより、定義されたユーザＩＤ以外でログインしようとすると、そのネットワークを切断する機能を持たせることが開示されている。

また、特開昭６３－２５３４５０号公報には、中央処理装置のオペレーティングシステムがユーザＩＤ、パスワード、回線アドレスをチェックすることにより、ディスク装置のファイルへの不正アクセス防止を行なうことが示されている。

さらに、ＩＢＭ社のＥＳＣＯＮインタフェースでは、上位装置が当該上位装置の論理アドレスをソースアドレスとしてフレームに格納し、送信してくることを利用して、記憶制御装置が事前に記憶制御装置に設定した論理アドレスとフレーム内の論理アドレスが一致するか否かをチェックする機能を設けている。

上述した従来技術は、上位論理層に１種類のレイヤを搭載するインタフェースを対象とした不正アクセス防止手段の域を出ないものである。

しかし、ＡＮＳＩＸ３Ｔ１１で標準化されたファイバチャネルは、ネットワーク形アーキテクチャであり、上位論理層にはＴＣＰ／ＩＰ、ＳＣＳＩ、ＥＳＣＯＮ、ＩＰＩ等の種々のレイヤを搭載可能である。すなわち、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、他のインタフェースと論理的に互換性を持ち、物理的に自由にアクセス可能である。特に、このファイバチャネルと、ディスクアレイ装置等の複数の記憶領域を有する記憶装置とを備えた記憶システムにおいては、上記記憶領域は多くの上位装置に共用される。したがって、従来の不正アクセス防止策では不十分であり、ユーザが意識したセキュリティ設定により、機密保持を行なう必要がある。

【０００３】

【特許文献１】特開昭６３－２５３４５０号

【発明の開示】

【発明が解決しようとする課題】

【０００４】

本発明は、ＡＮＳＩＸ３Ｔ１１で標準化されたファイバチャネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、この記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを拒絶する手段を持たなかった記憶制御装置に対し、上位装置からの不正なアクセスを防止するセキュリティ機能を設定出来る記憶制御装置及び記憶システムを提供することを目的とする。

【０００５】

さらに、本発明は、上位装置からの不正アクセス防止のために、アクセス可能な上位装置を容易に設定できる方式を持つ記憶制御装置及び記憶システムを提供することを目的とする。

【課題を解決するための手段】

【０００６】

本発明によれば、上記目的は、アクセス可能な上位装置の、上位装置を一意に識別するＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を当該記憶制御装置に設定し、上位装置から送られてくるフレーム内に格納されたＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報と比較し、アクセスの可否を決定することにより達成される。

【０００７】

上記目的を達成するための本発明の具体的な特徴は、上位装置から発行される、上位装置を一意に識別する情報であるＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を、パネル等を用いて入力し、入力情報を記憶制御装置の制御メモリに、制御テーブルとして格納する手段を有することである。この際、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有することが望ましい。

【０００８】

そして、上記制御テーブルを不揮発制御メモリに格納するようにすれば、万一の電源瞬断時にも管理情報を守ることができる。

【０００９】

さらに、本発明の具体的な特徴によれば、上位装置が立ち上がった後、上位装置がＮ＿

Ｐｏｒｔ＿Ｎａｍｅ情報を格納したフレームを記憶制御装置に対し発行し、記憶制御装置がこれを受領した際、記憶制御装置は既に設置され、保持されている上位装置を一意に識別するＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報と、受領したフレームに格納されたＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報とを比較する手段を有し、比較により一致した場合は、記憶制御装置は当該フレームの指示に基づく処理を継続し、
不一致の場合は、受領した当該フレームを拒絶するＬＳ＿ＲＪＴフレームを上位装置に返すようにしたことである。これにより、記憶制御装置は上位装置からの不正アクセスを抑止することができる。

【００１０】

さらに、本発明の具体的な特徴によれば、当該記憶制御装置が有する上位インタフェース（ポート）の物理的な数以上のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を設定する手段を有することである。すなわち、１ポートで複数のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を設定する手段を有することである。これにより、ファイバチャネルファブリック（Ｆａｂｒｉｃ）またはスイッチ接続時の論理パス多重構成に対応できる。

【００１１】

また、当該記憶制御装置の配下に、ディスクアレイ装置のような、多くの磁気ディスクボリュームを有し、複数のチャネルパスルートを有すシステムにおいては、チャネルパスルート毎に、当該記憶制御装置配下のＬＵＮ（ロジカルユニットナンバ）による論理ディスク領域、物理ボリューム領域、ＲＡＩＤグループによる論理ディスク領域等の記憶領域と、記憶制御装置のポート、上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報との対応付けを記憶制御装置内で管理する手段を有することである。これにより、ユーザは、記憶領域毎に、不正アクセスを防止することができ、木目細かいアクセス管理が可能となる。

【００１２】

さらに、本発明においては、記憶制御装置配下の記憶装置が磁気ディスク装置、
ディスクアレイ装置の代わりに、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらの各種ライブラリ装置の何れの場合でも、当該記憶制御装置は、アクセス可能な上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合はさらにドライブ、媒体の対応付けも行って、制御テーブルで管理、保持する手段を有し、フレーム受領の際にフレーム内の情報と制御テーブル内の情報を比較する手段を有し、
上位装置からの不正アクセスの防止を行うことができる。

【００１３】

さらに、本発明では、記憶制御装置が管理する情報を、パネル等を用いて設定する際、パスワードを入力する等により、管理情報を保護する手段を具備する。

【００１４】

これにより、ユーザは当該情報の不正な登録、不正な再設定を防止することができる。また、ユーザは管理情報の設定を行うだけで、容易に不正アクセスを防止可能であり、ユーザの負担が少ない。

【００１５】

なお、本発明において、記憶制御装置が管理する情報を設定する手段として、上述のように、パネル等を用いて設定する他に、上位装置のユティリティプログラムを用いて設定することも可能である。

【発明の効果】

【００１６】

本発明によって、ＡＮＳＩＸ３Ｔ１１で標準化されたファイバチャネルを上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、不正な上位装置からのアクセスを抑止することができるので、記憶装置内のデータの機密保護を行うことができる。

【００１７】

また、上位装置、記憶制御装置のポート、記憶領域を対応付けて上位装置からのアクセ

スを木目細かに管理できるので、記憶領域毎に用途を変える等、記憶装置をニーズに合わせて活用することができる。

【発明を実施するための最良の形態】

【００１８】

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。

【００１９】

まず、図１ないし図５を用いて、本発明の対象となるファイバチャネル及びそれを用いて構成した記憶システムについて説明する。

【００２０】

図１は、記憶制御装置配下の記憶装置がディスクアレイ装置の場合の記憶システムのハードウエア構成図である。図１において、１０、２０、３０は、データ処理を行う中央処理装置としての上位装置である。

【００２１】

４０は、本発明を実施したディスクアレイ装置の記憶制御装置である。図１に示すように、記憶制御装置４０は、上位装置１０、２０、３０との間のデータ転送を制御するためのＤＭＡ（ダイレクト　アクセス　メモリ）を含むプロトコルプロセッサであるファイバチャネル制御部４１、記憶制御装置全体を制御するマイクロプロセッサ４２、制御装置の動作を制御するマイクロプログラム及び制御用データを保存する制御メモリ４３、キャッシュへのデータの読み書きを制御するキャッシュ制御部４４、書き込みデータ及びディスクドライブからの読み出しデータを一時バッファリングしておくディスクキャッシュ４５、ディスクドライブとの間のデータ転送を制御するためのＤＭＡを含むプロトコルプロセッサであるデバイスインタフェース制御部４６、装置構成情報を記憶制御装置へ入力するパネル４７から構成されている。

【００２２】

５０は、記憶制御装置４０の配下にあるディスクアレイ装置である。ディスクアレイ装置５０は、上位装置のデータを格納する装置で、複数台の個別ディスクを冗長性を持つように配置構成したものである。

【００２３】

ディスクアレイ装置５０を構成するディスクは、論理的に分割し、分割した区画をそれぞれ異なるＲＡＩＤレベルに設定することができる。この区画をＲＡＩＤグループという。このＲＡＩＤグループをさらに論理的に分割したＳＣＳＩのアクセス単位である領域をＬＵ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ）といい、その領域は、各々、ＬＵＮ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）という番号を持つ。本実施の形態ではディスクアレイ装置５０は、ＬＵＮ０番のＬＵである、ＬＵ０（５１）とＬＵＮ１番のＬＵである、ＬＵ１（５２）の２個の領域を有する場合を示している。

【００２４】

なお、ＬＵの数は、図１に示す２個に限らずもっと多くてもよく、シングルターゲット機能の場合、ターゲット当り最大８個までＬＵを設定できる。

【００２５】

また、本実施の形態では、ＬＵなる記憶領域をアクセス単位としているが、アクセス単位とする記憶領域としては、物理ボリューム単位やＲＡＩＤグループ単位の記憶領域も可能である。

【００２６】

上位装置１０、２０、３０と記憶制御装置４０は、ファイバチャネル６０をインタフェースとし、ファブリック（Ｆａｂｒｉｃ）という装置を介して接続されている。

【００２７】

図１のシステムの動作を、上位装置１０が記憶制御装置４０経由でディスクアレイ装置５０とデータ転送を行う場合を例にとり、制御の流れ、データの流れを中心に説明する。

【００２８】

上位装置１０がアクセス要求を出すと、その要求を認識したファイバチャネル制御部４

１はマイクロプロセッサ４２に割り込み要求を発行する。マイクロプロセッサ４２は、上位装置からのコマンド情報及び本発明で必要な制御情報を、制御メモリ４３に格納する。

【００２９】

コマンド情報が、ライトコマンドの場合は、マイクロプロセッサ４２はファイバチャネル制御部４１にデータ転送を指示し、転送されたデータをキャッシュ制御部４４を経由してキャッシュ４５に格納する。上位装置１０に対しては、ファイバチャネル制御部４１がライト完了報告を行う。ライト完了報告後、マイクロプロセッサ４２がデバイスインタフェース制御部４６を制御し、ディスクアレイ装置５０に対し、データ及び冗長データを書き込む。この場合、一般のＲＡＩＤ５の動作においては、旧データ、旧パリティ及び新データに基いて新パリティを作成するが、本発明の制御によれば、マイクロプロセッサ４２が、デバイスインタフェース制御部４６及びキャッシュ制御部４４、制御メモリ４３、キャッシュ４５を用いて行なう。

【００３０】

一方、上位装置１０からコマンド情報として、リードコマンド情報を受けた場合は、マイクロプロセッサ４２は、デバイスインタフェース制御部４６に指示を出し、当該アクセス要求のデータブロックが格納されたディスクアレイ装置５０へアクセスしてデータを読み出し、キャッシュ制御部４４を経由してキャッシュ４５へデータを格納する。マイクロプロセッサ４２は、ファイバチャネル制御部４１に指示を出し、ファイバチャネル制御部４１は、キャッシュ４５に格納したデータを上位装置１０に転送し、転送後上位装置へリード完了報告を行なう。

【００３１】

次にファイバチャネル６０の特長を説明する。ファイバチャネルは最大１０ｋｍの距離で１００ＭＢ／ｓの転送が可能な高速インタフェースである。ファイバチャネルのアーキテクチャは転送元のバッファから転送先のバッファへデータを送るが、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、異なるネットワーク通信プロトコルを処理するオーバヘッドがなく、高速データ転送を実現している。上位論理層にはＴＣＰ／ＩＰ、ＳＣＳＩ、ＥＳＣＯＮ、ＩＰＩ等の種々のレイヤを搭載可能である。すなわち、他のインタフェースと論理的に互換性を持つ。複雑な装置間の接続／交換という機能はＦａｂｒｉｃと呼ぶ装置が行ない、論理パス多重構成を組むことが可能である。

【００３２】

ファイバチャネルがデータをやりとりする基本単位をフレームと言う。次に、このフレームについて、図２を用いて説明する。

【００３３】

図２に示すように、フレーム７０は、スタートオブフレームＳＯＦ（Ｓｔａｒｔ　Ｏｆ　Ｆｒａｍｅ）７１、フレームヘッダ７２、データフィールド７３、サイクリックリダンダンシチェックＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）７４及びエンドオブフレームＥＯＦ（Ｅｎｄ　Ｏｆ　Ｆｒａｍｅ）７５で構成される。

【００３４】

ＳＯＦ７１は、フレームの先頭に置く４バイトの識別子である。

【００３５】

ＥＯＦ７５は、フレームの最後につける４バイトの識別子で、ＳＯＦ７１とＥＯＦ７５によりフレームの境界を示す。ファイバチャネルではフレームがない時はアイドル（ｉｄｌｅ）という信号が流れている。

【００３６】

フレームヘッダ７２は、フレームタイプ、上位プロトコルタイプ、送信元と送信先のＮ＿Ｐｏｒｔ＿ＩＤ情報、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報等を含む。Ｎ＿Ｐｏｒｔ＿ＩＤはアドレスを表わし、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅはポートの識別子を表わす情報である。

【００３７】

データフィールド７３の先頭部には上位レイヤのヘッダを置くことができる。

【００３８】

これにデータそのものを運ぶペイロード部が続く。ＣＲＣ７４は、フレームヘッダとデータフィールドのデータをチェックするための、４バイトのチェックコードである。

【００３９】

上記フレームヘッダ７２のフォーマット８０を、図３に示す。フレームヘッダフォーマット８０において、デスティネーションアイデンティファイアＤ＿ＩＤ（Ｄｅｓｔｉｎａｔｉｏｎ　ＩＤ）８１はフレーム受け取り側のアドレス識別子であり、また、ソースアイデンティファイアＳ＿ＩＤ（Ｓｏｕｒｃｅ　ＩＤ）８２はフレーム送信側のＮ＿Ｐｏｒｔアドレス識別子であり、各々、Ｎ＿Ｐｏｒｔ＿ＩＤ情報等を含む。

【００４０】

次に図４を用いて、フレームを構成するデータフィールド７３のペイロードの１つである、ファイバチャネルプロトコルコマンドＦＣＰ＿ＣＭＮＤ（Ｆｉｂｒｅ　Ｃｈａｎｎｅｌ　Ｐｒｏｔｏｃｏｌ　ｆｏｒ　ＳＣＳＩ　Ｃｏｍｍａｎｄ）のペイロード９０の説明を行なう。

【００４１】

ＦＣＰロジカルユニットナンバＦＣＰ＿ＬＵＮ（ＦＣＰ　Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）フィールド９１には、コマンドを発行するロジカルユニット番号ＬＵＮが指定される。ＦＣＰコントロールＦＣＰ＿ＣＮＴＬ（ＦＣＰ　Ｃｏｎｔｒｏｌ）フィールド９２には、コマンド制御パラメータが指定される。

そして、ＦＣＰ コマンドデスクリプタブロックＦＣＰ＿ＣＤＢ（ＦＣＰ　Ｃｏｍｍａｎｄ　Ｄｉｓｃｒｉｐｔｏｒ　Ｂｌｏｃｋ）フィールド９３には、ＳＣＳＩコマンドディスクリプタブロック（ＳＣＳＩ　Ｃｏｍｍａｎｄ　Ｄｅｓｃｒｉｐｔｏｒ　Ｂｌｏｃｋ）が格納され、リードコマンドＲｅａｄ等のコマンド種類、ＬＵＮ等のアドレス、ブロック数が示される。ＦＣＰデータレングスＦＣＰ＿ＤＬ（ＦＣＰ　Ｄａｔａ　Ｌｅｎｇｔｈ）フィールド９４には、当該コマンドにより転送されるデータ量がバイト数で指定される。

【００４２】

以上のように構成されたフレームによってデータのやりとりが行われる。

【００４３】

フレームは機能に基づいてデータフレームとリンク制御フレームとに大別される。データフレームは、情報を転送するために用い、データフィールドのペイロード部に上位プロトコルで使用するデータ、コマンドを搭載する。

【００４４】

一方、リンク制御フレームは、一般に、フレーム配信の成功あるいは不成功を示すのに使われる。フレームを１個受領したことを示したり、ログインする場合に転送に関するパラメータを通知したりするフレーム等がある。

【００４５】

次に、図５を用いて、「シーケンス」について説明する。ファイバチャネルにおけるシーケンスは、あるＮ＿Ｐｏｒｔから別のＮ＿Ｐｏｒｔへ、一方向に転送される関連するデータフレームの集まりのことを言い、ＳＣＳＩのフェーズに相当する。シーケンスの集まりをエクスチェンジと呼ぶ。例えばコマンドを発行して、そのコマンドの終了までに、そのコマンド実行のためにやりとりされるシーケンスの集まり（コマンド発行、データ転送、終了報告）がエクスチェンジとなる。このように、エクスチェンジはＳＣＳＩのＩ／Ｏに相当する。

【００４６】

図５（ａ）、（ｂ）及び（ｃ）は、それぞれ、ログインシーケンス（１００）、リードコマンドシーケンス（１１０）及びライトコマンドシーケンス（１２０）を示す。

【００４７】

ファイバチャネルインタフェースでは、上位装置がデバイスに対し、通信パラメータを含むポートログインＰＬＯＧＩ（Ｎ＿Ｐｏｒｔ　Ｌｏｇｉｎ）フレームを送り、デバイス

がこれを受け付けることで通信が可能となる。これをログインと呼ぶ。図５（ａ）に、ログインシーケンス（１００）を示す。

【００４８】

図５（ａ）のログインシーケンス（１００）において、まず、シーケンス１０１で、上位装置はデバイスに対し、ＰＬＯＧＩフレームを送り、ログインの要求を行なう。デバイスはアクノレッジＡＣＫ（Ａｃｋｎｏｗｌｅｄｇｅ）フレームを上位装置に送り、ＰＬＯＧＩフレームを受け取ったことを知らせる。

【００４９】

次いで、シーケンス１０２において、デバイスは、ログイン要求を受け付ける場合はアクセプトＡＣＣ（Ａｃｃｅｐｔ）フレームを、要求を拒絶する場合はリンクサービスリジェクトＬＳ－ＲＪＴ（Ｌｉｎｋ　Ｓｅｒｖｉｃｅ　Ｒｅｊｅｃｔ）フレームを、それぞれ、上位装置に送る。

【００５０】

次に、図５（ｂ）のリードコマンドのシーケンス（１１０）を説明する。

【００５１】

シーケンス１１１において、上位装置はデバイスに対し、ＦＣＰ＿ＣＭＮＤフレームを送り、リード要求を行なう。デバイスはＡＣＫフレームを上位装置に送る。

【００５２】

シーケンス１０２では、デバイスは、ＦＣＰトランスファレディＦＣＰ＿ＸＦＥＲ＿ＲＤＹ（ＦＣＰ　Ｔｒａｎｓｆｅｒ　Ｒｅａｄｙ）フレームを上位装置に送り、データ転送の準備ができたことを知らせる。上位装置はＡＣＫフレームをデバイスに送る。

【００５３】

シーケンス１１３に進み、デバイスはＦＣＰデータ（ＦＣＰ＿ＤＡＴＡ）フレームを上位装置に送り、データを転送する。上位装置はＡＣＫフレームをデバイスに送る。

【００５４】

次のシーケンス１１４では、デバイスはＦＣＰ＿ＲＳＰフレームを上位装置に送り、データの転送が正常終了したことを知らせる。上位装置はＡＣＫフレームをデバイスに送る。

【００５５】

次に、図５（ｃ）のライトコマンドのシーケンス（１２０）を説明する。

【００５６】

シーケンス１２１において、上位装置はデバイスに対し、ＦＣＰ＿ＣＭＮＤフレームを送り、ライト要求を行なう。デバイスはＡＣＫフレームを上位装置に送る。

【００５７】

次いで、シーケンス１２２において、デバイスはＦＣＰ＿ＸＦＥＲ＿ＲＤＹフレームを上位装置に送り、データ書き込みが可能であることを知らせる。上位装置はＡＣＫフレームをデバイスに送る。

【００５８】

さらに、シーケンス１２３において、上位装置はＦＣＰ＿ＤＡＴＡフレームをデバイスに送り、データを転送する。デバイスはＡＣＫフレームを上位装置に送る。

【００５９】

最後に、シーケンス１２３において、デバイスは、ＦＣＰレスポンスＦＣＰ＿ＲＳＰ（ＦＣＰ　Ｒｅｓｐｏｎｓｅ）フレームを上位装置に送り、データの受け取りが正常終了したことを知らせる。上位装置はＡＣＫフレームをデバイスに送る。

【００６０】

以上、図１ないし図５によって、一般的なシステム構成、フォーマット及びシーケンスを説明したが、以下、本発明によるセキュリティチェックについて説明する。

【００６１】

初めに、ＰＬＯＧＩ時におけるＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を用いたセキュリティチェックについて、説明を行なう。

【００６２】
本発明では、図１において、まず、上位装置１０、２０、３０の立ち上がる以前に、ユーザは記憶制御装置４０のマイクロプロセッサ４２にアクセス可能な上位装置のリストを設定する。すなわち、上位装置を識別できるＮ＿Ｐｏｒｔ＿Ｎａｍｅ、Ｎ＿Ｐｏｒｔ＿ＩＤ等の情報を、パネル４７を用いて入力する。この際、パネルへの入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化できる。
【００６３】
パスワードを入力し、既に設定したパスワードとの一致が図られた場合、記憶制御装置のポート毎にアクセス可能な上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を入力し、入力情報を制御テーブルに格納する。
【００６４】
いま、例として、上位装置１０、２０はディスクアレイ装置５０にアクセス可能、上位装置３０はディスクアレイ装置５０にはアクセス不可能とし、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅを、上位装置１０はＨＯＳＴＡ、上位装置２０はＨＯＳＴＢ、上位装置３０はＨＯＳＴＣとし、記憶制御装置４０のファイバチャネル制御部４１のポートをＣＴＬ０Ｐ０とした場合、ログイン要求制御テーブル１３０は、図６のようになる。
【００６５】
図６に示すこのログイン要求制御テーブル１３０を、不揮発メモリ上に設定することにより、万一の電源瞬断時にも管理情報を守ることができる。
【００６６】
また、ログイン要求制御テーブル１３０に格納した情報は、電源を切断した場合はハードディスク領域５０へ格納する。または情報の更新時にメモリ４３とディスク５０へ反映を行なう。これにより記憶制御装置４０は、当該情報を再設定されるまで恒久的に保持することができる。
【００６７】
なお、ファイバチャネルにおいてノードやポートの識別に使用される自ノード情報として、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅの他に、Ｎ＿Ｐｏｒｔ＿ＩＤがあるが、Ｎ＿Ｐｏｒｔ＿ＩＤは変更される可能性があり、ユーザが管理する数値ではないため、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報をセキュリティのためのチェック対象とするのが望ましい。
【００６８】
次に、図１及び図７を用いて上位装置のログイン要求に対する記憶制御装置のフレーム処理手順の説明を行なう。
【００６９】
（ステップＳ７１）
上位装置１０、２０、３０が立ち上がり、各々、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報を格納したログイン要求フレームであるＰＬＯＧＩフレームを発行する。記憶制御装置４０のマイクロプロセッサ４２は、当該フレームを受領すると、まずこのフレームを受領したことを示すＡＣＫフレームを各上位装置に返す。
【００７０】
（ステップＳ７２）
そしてマイクロプロセッサ４２は、当該フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を切り出し、そのＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報が、既に設定され、保持されている制御テーブル内のＮ＿Ｐｏｒｔ＿Ｎａｍｅリストに登録されているかどうか、比較を行なう。
【００７１】
（ステップＳ７３）（ステップＳ７４）（ステップＳ７５）
上位装置１０、２０の発行した当該フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報は、制御テーブル内に登録されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報と一致するため、記憶制御装置４０のマイクロプロセッサ４２は、上位装置１０、２０に対してはログイン要求を受け付けた印として、ＡＣＣフレームを返し、ログイン処理を続行する。

【００７２】
（ステップＳ７３）（ステップＳ７６）
一方、上位装置３０の発行した当該フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報は、制御テーブル内に登録されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報と一致しないため、記憶制御装置４０のマイクロプロセッサ４２は、上位装置３０に対しては接続を拒絶するリジェクトパラメータをいれたＬＳ＿ＲＪＴフレームを返す。
【００７３】
以上のように、記憶制御装置４０が、ログイン要求制御テーブル１３０を用いて、上位装置と記憶制御装置のポートの対応付けを管理することにより、ユーザはポート毎に上位装置からの不正アクセスを抑止することができ、セキュリティが保持できる。
【００７４】
次に、本発明において、ディスクアレイ装置の記憶領域であるＬＵＮ毎に、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ情報を用いてセキュリティチェックを実施する方法について説明する。
【００７５】
本発明では、まず上位装置１０、２０、３０の立ち上がる以前に、記憶制御装置４０のマイクロプロセッサ４２に、ＬＵＮ毎にアクセス可能な上位装置のリストを設定する。上位装置を識別できるＮ＿Ｐｏｒｔ＿Ｎａｍｅ、Ｎ＿Ｐｏｒｔ＿ＩＤ等の情報を、パネル４７を用いて入力する。この際、パネル４７への入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化することができる。
【００７６】
パスワードを入力し、既に設定したパスワードとの一致が図られた場合、ＬＵＮ毎に記憶制御装置のポート及びアクセス可能な上位装置のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を入力し、入力情報を制御テーブルに格納する。
【００７７】
ＬＵ０（５１）は、上位装置１０から記憶制御装置４０のファイバチャネル制御部４１のポート経由でアクセス可能、ＬＵ１（５２）は、上位装置２０から記憶制御装置４０のファイバチャネル制御部４１のポート経由でアクセス可能とし、
Ｎ＿Ｐｏｒｔ＿Ｎａｍｅを、上位装置１０はＨＯＳＴＡ、上位装置２０はＨＯＳＴＢ、記憶制御装置４０のファイバチャネル制御部４１のポートをＣＴＬ０Ｐ０、とした場合、Ｉ／Ｏ要求制御テーブル１４０は、図８のようになる。
【００７８】
図８に示すこのＩ／Ｏ要求制御テーブル１４０は不揮発メモリ上に設定すると、
万一の電源瞬断時にも管理情報を守ることができる。
【００７９】
また、図８のＩ／Ｏ要求制御テーブル１４０に格納した情報は、電源を切断した場合は、ハードディスク領域５０へ格納する。または情報の更新時にメモリ４３とディスク５０へ反映を行なう。これにより記憶制御装置４０は当該情報を再設定されるまで恒久的に保持することができる。
【００８０】
本実施例ではチャネルパスルートは１通りであるが、複数のチャネルパスルートを有するシステムにおいても同様である。
【００８１】
以下に図１及び図９を用いて、上位装置のＩ／Ｏ要求に対する記憶制御装置のフレーム処理手順の説明を行なう。上記の例ではＰＬＯＧＩ時にセキュリティチェックを行なったが、本実施の形態では、各ＳＣＳＩコマンド毎にチェックを行なう。
【００８２】
（ステップＳ９１）
上位装置１０がＬＵ０（５１）にＩ／Ｏ要求を出したい場合、上位装置１０は記憶制御装置４０に対し、ＳＣＳＩ　ＣＤＢを格納したフレームを発行する。記憶制御装置４０がこのフレームを受領した場合、まず、このフレームを受領したことを示すＡＣＫフレームを

上位装置１０に返す。
【００８３】
（ステップＳ９２）
そしてマイクロプロセッサ４２は、当該フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報及びＣＤＢ内のＬＵＮ番号を切り出し、そのＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報及びＬＵＮ番号が、当該マイクロプロセッサ４２に既に設定され保持されている制御テーブル内のリストに登録されているかどうか、比較を行なう。
【００８４】
（ステップＳ９３）（ステップＳ９４）（ステップＳ９５）
管理テーブル内には、「上位装置１０は、ＬＵ０（５１）をアクセス可能である」と登録されているため、記憶制御装置４０のマイクロプロセッサ４２はコマンドを受領し、Ｉ／Ｏ処理を継続する。
【００８５】
（ステップＳ９１）
一方、上位装置２０が記憶制御装置４０にＬＵ０（５１）のＩ／Ｏ要求フレームを発行し、記憶制御装置４０がこのＳＣＳＩ　ＣＤＢを格納したフレームを受領した場合、マイクロプロセッサ４２は、まずこのフレームを受領したことを示すＡＣＫフレームを上位装置２０に返す。
【００８６】
（ステップＳ９２）
そしてマイクロプロセッサ４２は、当該フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報及びＣＤＢ内のＬＵＮ番号を切り出し、そのＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報及びＬＵＮ番号が、管理テーブル内にあるかどうかの検索を行なう。
【００８７】
（ステップＳ９３）（ステップＳ９６）
検索を行なった結果、管理テーブル内に、該当するＬＵＮおよびＮ＿Ｐｏｒｔ＿Ｎａｍｅの組合わせが存在しないため、記憶制御装置４０のマイクロプロセッサ４２は、上位装置２０にＬＳ＿ＲＪＴフレームを送って、Ｉ／Ｏ要求を拒絶する。
【００８８】
こうして記憶制御装置は不正なアクセスを防止することができる。
【００８９】
ここではログイン及びＩ／Ｏ要求フレームを取り上げたが、これら以外の他の上位装置フレームに格納されているＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報を比較してもよい。
【００９０】
なお、ファイバチャネル接続記憶制御装置配下の記憶装置がディスクアレイ装置に限らず、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置である場合にも本発明を適用できる。
【００９１】
記憶制御装置配下の記憶装置が光ディスクライブラリ装置の場合に本発明を適用した場合の概要を図１０を用いて説明する。１５０は記憶制御装置４０配下の光ディスクライブラリ装置であり、１５１は光ディスクドライブ、１５２から１５６は光ディスクの媒体である。
【００９２】
ユーザは上位装置１０、２０、３０が立ち上る前にパネルを使用して、媒体、ドライブ、ポートとＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報との対応付けを設定し、上位装置のアクセス権限をマイクロプログラムに保持しておく。
【００９３】
媒体１５２、１５３、１５４は、上位装置１０からアクセス可能、媒体Ｄ１５５、Ｅ１５６は上位装置２０からアクセス可能とし、Ｎ＿Ｐｏｒｔ＿Ｎａｍｅを上位装置１０はＨＯＳＴＡ、上位装置２０はＨＯＳＴＢ、記憶制御装置４０のポートをＣＴＬ０Ｐ０、光デ

ィスクドライブＡ１５１をＤＲＩＶＥ０、媒体Ａ１５２、Ｂ１５３、Ｃ１５４、Ｄ１５５、Ｅ１５６を各々ＭＥＤＡ、ＭＥＤＢ、ＭＥＤＣ、ＭＥＤＤ、ＭＥＤＥ、とした場合、要求制御テーブル１６０は、図１１のようになる。

【００９４】

各上位装置がＩ／Ｏ要求フレームを発行した際、フレームを構成するペイロード内のＣＤＢにボリューム情報が格納されているため、記憶制御装置４０は当該フレームを受領した際、フレーム内のＮ＿Ｐｏｒｔ＿Ｎａｍｅ情報及びペイロード内の媒体識別子を，当該記憶制御装置４０に既に設定され、保持されている制御テーブルと比較を行なえばよい。

このように、本発明を応用することによって、

記憶制御装置は上位装置からの不正アクセスを防止可能である。

【図面の簡単な説明】

【００９５】

【図１】本発明の実施の形態を示す構成図である。

【図２】フレームのフォーマット図である。

【図３】図２で示したフレームを構成するフレームヘッダのフォーマット図である。

【図４】図２で示したフレームの一つであるＦＣＰ＿ＣＭＮＤのペイロードのフォーマット図（ａ）及び当該ペイロードを構成するＦＣＰ＿ＣＤＢのフォーマット図（ｂ）である。

【図５】上位装置とデバイスがデータフレームのやりとりを行なう際の、ログイン時のシーケンス図（ａ）、リードコマンド時のシーケンス図（ｂ）及びライトコマンド時のシーケンス図（ｃ）である。

【図６】記憶制御装置が上位装置を管理する制御テーブルを示した図である。

【図７】記憶制御装置が上位装置からのログイン要求時に実行するフレーム処理のフローチャートである。

【図８】記憶制御装置が記憶領域を管理する制御テーブルを示した図である。

【図９】記憶制御装置がホストからのＩ／Ｏ要求時に実行するフレーム処理のフローチャートである。

【図１０】記憶制御装置配下の記憶装置が、光ディスクライブラリの場合を示す構成図である。

【図１１】図１０に示す記憶制御装置が管理する制御テーブルを示した図である。

【符号の説明】

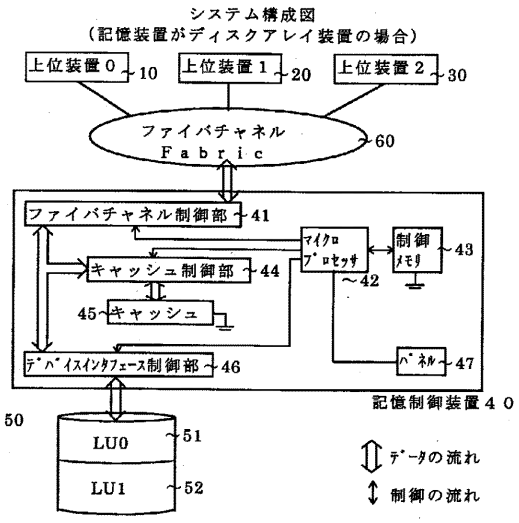
【００９６】

１０、２０，３０…上位装置、４０…記憶制御装置、４１…ファイバチャネル制御部、４２…マイクロプロセッサ、４３…制御メモリ、４４…キャッシュ制御部、４５…キャッシュ、４６…デバイスインタフェース制御部、４７…パネル、５０…ディスクアレイ装置、５１…ロジカルユニット０、５２…ロジカルユニット１、６０…ファイバチャネル、７０…フレーム、７１…スタートオブフレームＳＯＦ（Ｓｔａｒｔ Ｏｆ Ｆｒａｍｅ）、７２…フレームヘッダ、７３…データフィールド、７４…サイクリックリダンダンシチェックＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）、７５…エンドオブフレームＥＯＦ（Ｅｎｄ Ｏｆ Ｆｒａｍｅ）、８０…フレームヘッダのフォーマット、８１…デスティネーションアイデンティファイアＤ＿ＩＤ（Ｄｅｓｔｉｎａｔｉｏｎ ＩＤ）、８２…ソースアイデンティファイアＳ＿ＩＤ（Ｓｏｕｒｃｅ ＩＤ）、９０…ファイバチャネルプロトコルコマンドＦＣＰ＿ＣＭＮＤペイロード（Ｆｉｂｒｅ Ｃｈａｎｎｅｌ Ｐｒｏｔｏｃｏｌ ｆｏｒ ＳＣＳＩ Ｃｏｍｍａｎｄ）、９１…ファイバチャネルプロトコルロジカルユニットナンバＦＣＰ＿ＬＵＮ（ＦＣＰ Ｌｏｇｉｃａｌ Ｕｎｉｔ Ｎｕｍｂｅｒ）、９２…ファイバチャネルプロトコルコントロールＦＣＰ＿ＣＮＴＬ（ＦＣＰ Ｃｏｎｔｒｏｌ）、９３…ファイバチャネルプロトコルコマンドデスクリプタブロックＦＣＰ＿ＣＤＢ（ＦＣＰ Ｃｏｍｍａｎｄ Ｄｅｓｃｒｉｐｔｏｒ Ｂｌｏｃｋ）

、９４…ファイバチャネルプロトコルデータレングスＦＣＰ＿ＤＬ（ＦＣＰ　Ｄａｔａ　Ｌｅｎｇｔｈ）、１００…ログイン、１１０…リードコマンド、１２０…ライトコマンド、１３０…ログイン要求制御テーブル、１４０…磁気ディスクアレイＩ／Ｏ要求制御テーブル、１５０…光ディスクライブラリ、１６０…光ディスクライブラリＩ／Ｏ要求制御テーブル

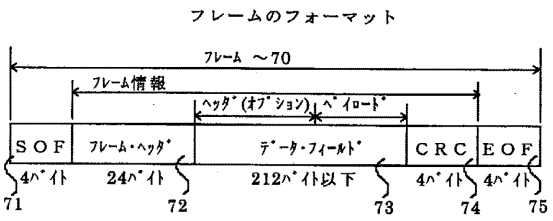
【図１】

【図１】



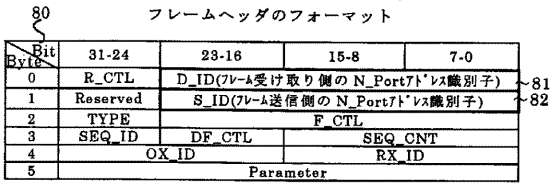
【図２】

【図２】



【図３】

【図３】

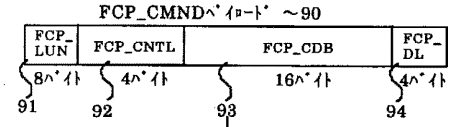


Ｒ＿ＣＴＬ：Routing Control、　Ｄ＿ＩＤ：Destination ID
Ｓ＿ＩＤ：Source ID、　ＴＹＰＥ：Data Structure Type
Ｆ＿ＣＴＬ：Frame Control、　ＳＥＱ＿ＩＤ：Sequence ID
ＤＦ＿ＣＴＬ：Data Field Control、　ＳＥＱ＿ＣＮＴ：Sequence Count
ＯＸ＿ＩＤ：Originator Exchange ID
ＲＸ＿ＩＤ：Responder Exchange ID

【図４】

【図４】

ＦＣＰ＿ＣＭＮＤペイロードのフォーマット



FCP_CDB93 のﾌｫｰﾏｯﾄ

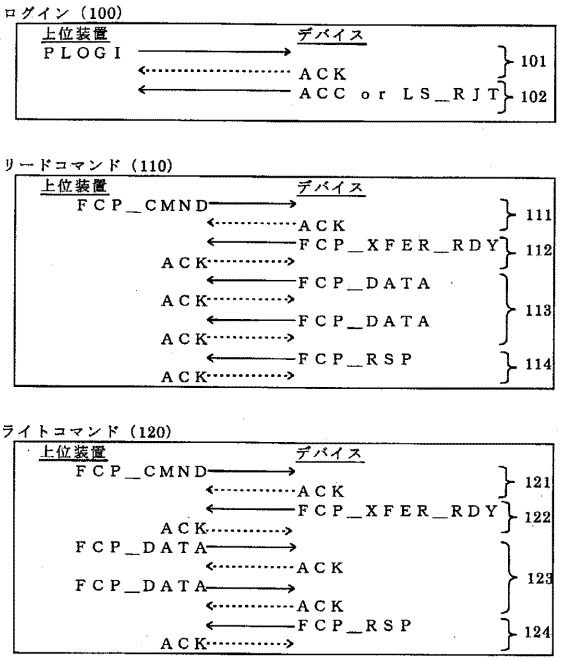
Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code							
1	Logical Unit Number			Logical Block Address(MSB)				
2	Logical Block Address							
3	Logical Block Address(LSB)							
4	Transfer Length							
5	Vendor Unique		Reserved				Flag	Link

FCP : Fibre Channel Protocol for SCSI, CMND : Command
LUN : Logical Unit Number, CNTL : Control
CDB : Command Descriptor Block , DL : Data Length

【図５】

【図５】

シーケンス



PLOGI : N_Port Login, ACK : Acknowledge
ACC : Accept, LS_RJT: Link Service Reject
FCP : Fibre Channel Protocol for SCSI, CMND : Command
XFER_RDY : Transfer Ready, DATA : Data, RSP : Response

【図６】

【図６】

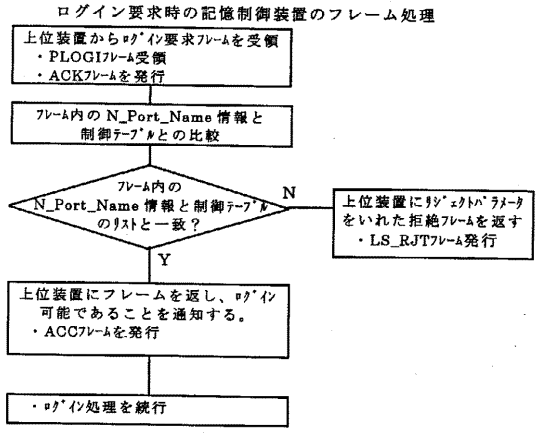
制御テーブル 130

上位装置の N＿Ｐｏｒｔ＿Ｎａｍｅ	記憶制御装置の 上位ｲﾝﾀﾌｪｰｽ(ﾎﾟｰﾄ)
HOSTA	ＣＴＬ０Ｐ０
HOSTB	ＣＴＬ０Ｐ０

【図７】

【図７】

ログイン要求時の記憶制御装置のフレーム処理



【図８】

【図８】

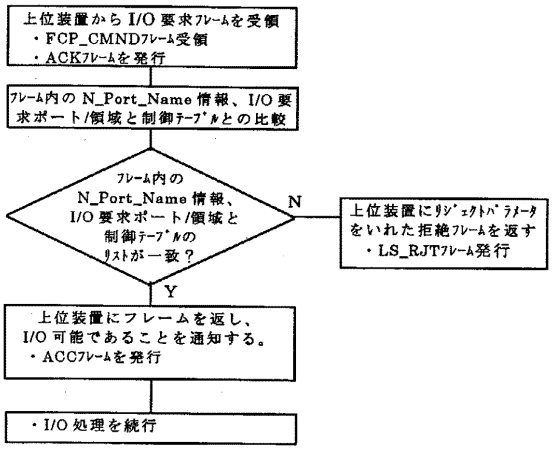
制御テーブル 140

記憶領域 ＬＵ	上位装置の Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ	記憶制御装置の 上位ｲﾝﾀﾌｪｰｽ(ﾎﾟｰﾄ)
ＬＵＯ	HOSTA	ＣＴＬ０Ｐ０
ＬＵ１	HOSTB	ＣＴＬ０Ｐ０

【図９】

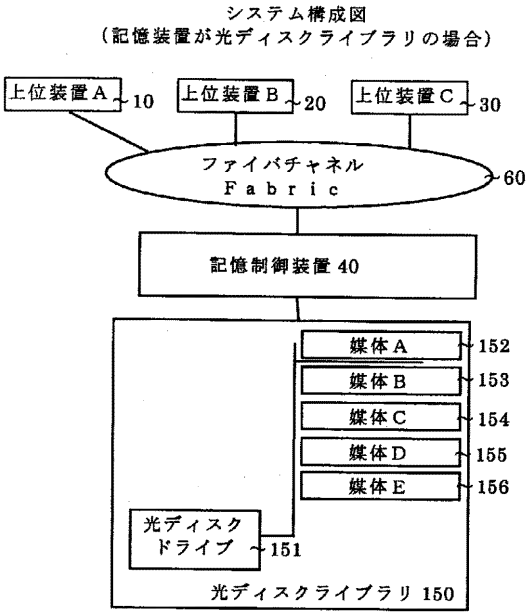
【図９】

Ｉ／Ｏ要求時の記憶制御装置のフレーム処理



【図１０】

【図 10】



【図１１】

【図 11】

制御テーブル 160

記憶領域 光ﾃﾞｨｽｸ媒体	光ﾃﾞｨｽｸ ﾄﾞﾗｲﾌﾞ	上位装置の N_Port_Name	記憶制御装置の 上位ｲﾝﾀﾌｪｰｽ(ﾎﾟｰﾄ)
ＭＥＤＡ	ＤＲＩＶＥ０	HOSTA	ＣＴＬ０Ｐ０
ＭＥＤＢ	ＤＲＩＶＥ０	HOSTA	ＣＴＬ０Ｐ０
ＭＥＤＣ	ＤＲＩＶＥ０	HOSTA	ＣＴＬ０Ｐ０
ＭＥＤＤ	ＤＲＩＶＥ０	HOSTB	ＣＴＬ０Ｐ０
ＭＥＤＥ	ＤＲＩＶＥ０	HOSTB	ＣＴＬ０Ｐ０

フロントページの続き

(72)発明者　岩崎　秀彦
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　佐藤　雅彦
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　村岡　健司
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　高本　賢一
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　小林　正明
神奈川県小田原市国府津２８８０番地　株式会社日立製作所ストレージシステム事業部内

Ｆターム(参考) 5B014 EB04　HA00
5B017 AA07　BB06
5B065 BA01　PA02　PA04　PA13