(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2008-250779
(P2008-250779A)
(43)公開日　平成20年10月16日(2008.10.16)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 3/06	(2006.01)	G06F	3/06	304H	5B017
G06F 21/24	(2006.01)	G06F	3/06	540	5B065
		G06F	12/14	540A	

審査請求 未請求　請求項の数 21　ＯＬ　（全 27 頁）

(21)出願番号　特願2007-92478(P2007-92478)
(22)出願日　平成19年3月30日(2007.3.30)

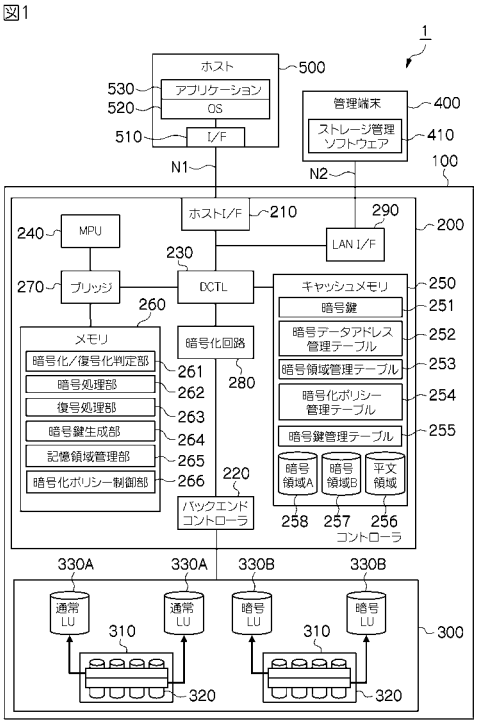
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100093861
弁理士　大賀　眞司
(72)発明者　川上　順彦
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5B017 AA01　BA07　CA07　CA16
5B065 BA01　PA16

(54)【発明の名称】暗号機能を備えた記憶制御装置、データ暗号化方法及び記憶システム

(57)【要約】
【課題】ホスト等から受信したデータを、ユーザの所望する暗号化ポリシーを適用することができることを目的とした、暗号機能を備えた記憶制御装置、データ暗号化方法及び記憶システムを提供することにある。
【解決手段】ホスト装置からのデータを記憶するための記憶装置と、記憶装置に記憶されるデータの入出力を制御するためのコントローラと、を備える記憶制御装置において、コントローラは、データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理部と、暗号機能に関する属性の設定情報に基づいて、ホスト装置からのデータと記憶装置に記憶されるデータとの暗号化を行う暗号化実行部と、を備えることとする。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
ホスト装置からのデータを記憶するための記憶装置と、前記記憶装置に記憶されるデータの入出力を制御するためのコントローラと、を備える記憶制御装置において、
前記コントローラは、
データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理部と、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータと前記記憶装置に記憶されるデータとの暗号化を行う暗号化実行部と、を備える
ことを特徴とする記憶制御装置。
【請求項２】
前記コントローラは、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うか否かの判定を行う暗号化判定部をさらに備える
ことを特徴とする請求項１記載の記憶制御装置。
【請求項３】
前記記憶装置は、複数備えられ、
前記データは、
複数の前記記憶装置が提供する複数の記憶領域又は複数の前記記憶装置が動的に提供する複数の記憶領域に記憶される
ことを特徴とする請求項１記載の記憶制御装置。
【請求項４】
前記暗号化実行部は、
前記記憶装置に記憶されるデータと関連するデータを、前記記憶装置に記憶されるデータの暗号化を行う際に暗号化を行う
ことを特徴とする請求項１記載の記憶制御装置。
【請求項５】
前記暗号化判定部は、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うと判定すると、
暗号化を行うための前記記憶領域の情報を検索して判定し、
前記暗号化を行うための記憶領域に関連する記憶領域の情報を検索して判定する
ことを特徴とする請求項３記載の記憶制御装置。
【請求項６】
前記設定情報管理部は、
前記暗号化を行うための記憶領域及び当該記憶領域に関連する記憶領域を管理する領域管理テーブル又は前記記憶領域に記憶されるデータのアドレス及び前記記憶領域に関連する記憶領域に記憶されるデータのアドレスを管理するアドレス管理テーブルを有する、
ことを特徴とする請求項３記載の記憶制御装置。
【請求項７】
前記設定情報管理部は、
前記暗号化を行うための記憶領域及び当該記憶領域に関連する記憶領域を暗号化又は復号化を行うために設けられる暗号鍵の管理を行う暗号鍵管理テーブルを有する、
ことを特徴とする請求項３記載の記憶制御装置。
【請求項８】
ホスト装置からのデータを記憶するための記憶装置と、前記記憶装置に記憶されるデータの入出力を制御するためのコントローラと、を備える記憶制御装置のデータ暗号化方法において、
前記コントローラでは、

データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理ステップと、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータと前記記憶装置に記憶されるデータとの暗号化を行う暗号化実行ステップと、を備える
ことを特徴とするデータ暗号化方法。
【請求項９】
前記コントローラでは、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うか否かの判定を行う暗号化判定ステップをさらに備える
ことを特徴とする請求項８記載のデータ暗号化方法。
【請求項１０】
前記記憶装置は、複数備えられ、
前記データは、
複数の前記記憶装置が提供する複数の記憶領域又は複数の前記記憶装置が動的に提供する複数の記憶領域に記憶される
ことを特徴とする請求項８記載のデータ暗号化方法。
【請求項１１】
前記暗号化実行ステップでは、
前記記憶装置に記憶されるデータと関連するデータを、前記記憶装置に記憶されるデータの暗号化を行う際に暗号化を行う
ことを特徴とする請求項８記載のデータ暗号化方法。
【請求項１２】
前記暗号化判定ステップでは、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うと判定すると、
暗号化を行うための前記記憶領域の情報を検索して判定し、
前記暗号化を行うための記憶領域に関連する記憶領域の情報を検索して判定する
ことを特徴とする請求項１０記載のデータ暗号化方法。
【請求項１３】
前記設定情報管理ステップでは、
前記暗号化を行うための記憶領域及び当該記憶領域に関連する記憶領域を管理する領域管理テーブル又は前記記憶領域に記憶されるデータのアドレス及び前記記憶領域に関連する記憶領域に記憶されるデータのアドレスを管理するアドレス管理テーブルを有し、
前記領域管理テーブル又は前記アドレス管理テーブルに基づいて前記暗号機能に関する属性の設定情報を管理する
ことを特徴とする請求項１０記載のデータ暗号化方法。
【請求項１４】
前記設定情報管理ステップでは、
前記暗号化を行うための記憶領域及び当該記憶領域に関連する記憶領域を暗号化又は復号化を行うために設けられる暗号鍵の管理を行う暗号鍵管理テーブルを有し、
前記暗号鍵管理テーブルに基づいて前記暗号機能に関する属性の設定情報を管理する
ことを特徴とする請求項１０記載のデータ暗号化方法。
【請求項１５】
ホスト装置からのデータを記憶するための記憶装置に記憶されるデータの入出力を制御する記憶制御装置を備える記憶システムにおいて、
前記記憶制御装置は、
データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理部と、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータと前記

記憶装置に記憶されるデータとの暗号化を行う暗号化実行部と、を備える
ことを特徴とする記憶システム。
【請求項１６】
前記記憶制御装置は、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うか否かの判定を行う暗号化判定部をさらに備える
ことを特徴とする請求項１５記載の記憶システム。
【請求項１７】
前記記憶装置は、複数備えられ、
前記データは、
複数の前記記憶装置が提供する複数の記憶領域又は複数の前記記憶装置が動的に提供する複数の記憶領域に記憶される
ことを特徴とする請求項１５記載の記憶システム。
【請求項１８】
前記暗号化実行部は、
前記記憶装置に記憶されるデータと関連するデータを、前記記憶装置に記憶されるデータの暗号化を行う際に暗号化を行う
ことを特徴とする請求項１５記載の記憶システム。
【請求項１９】
前記暗号化判定部は、
前記暗号機能に関する属性の設定情報に基づいて、前記ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うと判定すると、
暗号化を行うための前記記憶領域の情報を検索して判定し、
前記暗号化を行うための記憶領域に関連する記憶領域の情報を検索して判定する
ことを特徴とする請求項１７記載の記憶システム。
【請求項２０】
前記設定情報管理部は、
前記暗号化を行うための記憶領域及び当該記憶領域に関連する記憶領域を管理する領域管理テーブル又は前記記憶領域に記憶されるデータのアドレス及び前記記憶領域に関連する記憶領域に記憶されるデータのアドレスを管理するアドレス管理テーブルを有する、
ことを特徴とする請求項１７記載の記憶システム。
【請求項２１】
前記設定情報管理部は、
前記暗号化を行うための記憶領域及び当該記憶領域に関連する記憶領域を暗号化又は復号化を行うために設けられる暗号鍵の管理を行う暗号鍵管理テーブルを有する、
ことを特徴とする請求項１７記載の記憶システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号機能を備えた記憶制御装置、データ暗号化方法及び記憶システムに関する。
【背景技術】
【０００２】
企業等の組織では、大量のデータを管理するために、ホスト装置（以下、ホストという）とは別に構成された記憶制御装置を用いている。このような記憶制御装置は、例えば、ハードディスクドライブ等の記憶装置を多数内蔵しており、大容量の記憶領域をホストに提供する。
【０００３】
記憶制御装置には、例えば、個人の住所、氏名等の個人情報や信用情報等のような各種

の重要な秘密にされるべき情報が保存されている。従って、前述の重要情報を安全に管理して、不正なアクセス等を防止するための技術が求められている。

【０００４】

前述のような重要なデータを保護するために、暗号化技術を用いて記憶制御装置を管理する方法が特許文献１に開示されている。

【０００５】

特許文献１では、ホストとの通信を制御するインターフェースの内部において、ホストに接続されるホストインターフェースと転送制御部との間に暗号処理部を設ける。そしてホストから受信したデータは、暗号処理部によって暗号化されてから、ハードディスクドライブに書き込まれる。このように特許文献１の技術では、データの暗号化を記憶制御装置の内部で行うことにより、記憶制御装置内に格納されるデータのセキュリティを確保することができる。加えて特許文献１によれば、大量の重要データを保存しておく記憶制御装置において、データを暗号化して記憶させることにより、万一データが所有者でない第三者に漏洩した場合にも、当該データに対する不正な使用をデータの暗号化により防止することができる。

【特許文献１】特開２００５－３２２２０１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

全てのホストから受信したデータに対して、記憶制御装置の初期導入時から暗号機能を有効化して運用していた場合には、全てのデータを暗号化して保護することができた。しかしながら、暗号化するデータと暗号化しない通常のデータ（以下、平文データという）とを共存させて記憶制御装置を運用する場合や、記憶制御装置に関する機能を初期導入後に追加、又は、記憶制御装置自体のアップグレードを行う等により、途中から暗号機能を有効化して記憶制御装置の運用する場合には、予め保存される全てのデータを暗号化して保護することは難しい。

【０００７】

また、前述の記憶制御装置の運用においては、既に平文データとして管理していたところに運用途中で暗号機能を有効化することで、暗号機能を有効化した後に扱うデータについては暗号化によるデータ保護をサポートできるが、暗号機能を有効化する前に扱われたデータについては暗号化によるデータ保護の対象とならない。このため、前述の記憶制御装置の運用では、データ漏洩の危険性が残されてしまうこととなる。

【０００８】

例えば、スナップショット（Snapshot）技術のような時系列的に複数世代のバックアップデータを保存しておく際に、記憶制御装置が平文データをプライマリデータとして保存していた場合には、バックアップデータも平文データで保存されるのが通常である。ある時点で記憶制御装置の運用ポリシーを変更して暗号機能を有効化した場合には、暗号機能を有効化した後の記憶制御装置が受信した平文データは暗号化処理が行われ、暗号化されたデータとして保存される。そして、この暗号化されたデータをバックアップする場合にも、暗号機能を有効化した時点から更新された分までに暗号化されたデータがバックアップデータとして保存されることとなる。しかし、暗号機能の有効化される前のバックアップデータに関しては、記憶制御装置内に平文データのまま保存されることとなる。

【０００９】

あるいは、ホスト等が使用するプライマリデータについては平文データのまま通常の運用を行い、バックアップデータのみ暗号化して運用するという方法も一般的に考えられる。また、記憶制御装置内でバックアップデータを暗号化して運用し、最終的にはバックアップデータをテープ等のメディアにバックアップして一旦保管しておき、災害対策等のために遠隔地へ運搬して運用する方法が考えられる。しかし、このようなデータを保存するメディアは可搬媒体であるため、可搬媒体を取り出して外に保管及び運搬等の扱いは、盗難や紛失等のデータ漏洩の危険性が高い。

【００１０】
加えて、記憶制御装置に保存するデータに対する暗号化の運用については、ユーザのセキュリティに対する意識のレベル、暗号化に関わるコスト及び記憶制御装置の処理性能等、ユーザのデータ保護に対する暗号化ポリシーに基づいて決定される。
【００１１】
そこで本発明は、ホスト等から受信したデータを、ユーザの所望する暗号化ポリシーを適用することができることを目的とした、暗号機能を備えた記憶制御装置、データ暗号化方法及び記憶システムを提供することにある。本発明のさらなる目的は、後述する実施形態の記載から明らかになるであろう。
【課題を解決するための手段】
【００１２】
上記課題を解決するために、本発明は、ホスト装置からのデータを記憶するための記憶装置と、記憶装置に記憶されるデータの入出力を制御するためのコントローラと、を備える記憶制御装置において、コントローラは、データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理部と、暗号機能に関する属性の設定情報に基づいて、ホスト装置からのデータと記憶装置に記憶されるデータとの暗号化を行う暗号化実行部と、を備えることを特徴とする。
【００１３】
この結果、本発明の記憶制御装置はデータを暗号化する機能を備える。暗号化されていないホスト装置からのデータと予め記憶装置に記憶されるデータとを暗号化することができる。
【００１４】
また、本発明は、ホスト装置からのデータを記憶するための記憶装置と、記憶装置に記憶されるデータの入出力を制御するためのコントローラと、を備える記憶制御装置のデータ暗号化方法において、コントローラでは、データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理ステップと、暗号機能に関する属性の設定情報に基づいて、ホスト装置からのデータと記憶装置に記憶されるデータとの暗号化を行う暗号化実行ステップと、を備えることを特徴とする。
【００１５】
この結果、本発明の記憶制御装置はデータを暗号化する機能を備える。暗号化されていないホスト装置からのデータと予め記憶装置に記憶されるデータとを暗号化することができる。
【００１６】
また、本発明は、ホスト装置からのデータを記憶するための記憶装置に記憶されるデータの入出力を制御する記憶制御装置を備える記憶システムにおいて、記憶制御装置は、データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理部と、暗号機能に関する属性の設定情報に基づいて、ホスト装置からのデータと記憶装置に記憶されるデータとの暗号化を行う暗号化実行部と、を備えることを特徴とする。
【００１７】
この結果、本発明の記憶制御装置はデータを暗号化する機能を備える。暗号化されていないホスト装置からのデータと予め記憶装置に記憶されるデータとを暗号化することができる。
【００１８】
また、本発明の記憶制御装置は、ユーザが暗号化ポリシーを設定するためのインターフェースを備えてユーザの所望する暗号化ポリシーを設定する手段を提供し、設定された暗号化ポリシーを記憶制御装置の設定情報として記憶しておく。また、記憶された暗号化ポリシーに基づいて、記憶制御装置が処理するデータに関わる暗号処理を自律的に実施する機能を備える。
【００１９】
ユーザは記憶制御装置の管理ソフトウェア、ホスト等上で稼働するＯＳ（Operating Sy

stem）やアプリケーション等を介して暗号化ポリシーの設定を行い、暗号機能の有効化、無効化等の設定を行う。また、設定とは別に通常の業務、運用におけるデータ処理による記憶制御装置とのデータの送受信を行う。

【００２０】

記憶制御装置は、設定された暗号化ポリシーに基づいて、送受信するデータの暗号処理及び復号処理を行い、必要に応じて既に記憶制御装置内に保存されているデータの暗号化を行う。暗号化の対象は、ＬＵ（Logical Unit）、ＲＡＩＤグループ、ディスクドライブ、装置内データ一時保存領域、キャッシュメモリ等の記憶領域であり、具体的には、指定されたＬＵのバックアップ領域等が含まれる。

【００２１】

そして、暗号化ポリシーが適用された時点で暗号処理設定がなされていれば、それ以降のホストからの入出力データを暗号化して処理すると共に、前記暗号化ポリシーの設定に基づいて前記暗号処理が開始される以前に記憶制御装置内に保存されていた平文データについても暗号化が必要である場合には暗号処理を行い、暗号データについて異なる暗号鍵による再暗号化、あるいは記憶領域の暗号化、データのコピーやバックアップに関する暗号化ポリシーを守るための処理を記憶制御装置が実施する。

【００２２】

なお、特に明示しないが、記憶制御装置は必要に応じて暗号データの復号処理についても実施するものとする。

【発明の効果】

【００２３】

本発明によると、記憶制御装置に設定された暗号化ポリシーを当該記憶制御装置に適用することによって、記憶制御装置の運用を変更した場合にも予め保存される全てのデータを記憶制御装置内で暗号化することができるため、ユーザが直接操作しないバックアップデータ等の各種データについても確実にデータを保護することができる。

【００２４】

また、記憶制御装置に暗号化ポリシーを設定する手段を提供することにより、記憶制御装置のユーザは、その時に必要な所望（記憶制御装置のデータ処理性能及び暗号機能を備えた記憶制御装置或いは運用するコスト及びデータの重要性等）のセキュリティレベルに基づいて暗号化されたデータの漏洩を防止することができる。

【発明を実施するための最良の形態】

【００２５】

以下、図面に基づき、本発明の実施の形態を説明する。図１に示すように、１は本実施の形態におけるストレージシステムの全体構成を示す説明図である。このストレージシステム１は、記憶システムであって、ストレージ装置１００が通信ネットワークＮ１を介してホスト５００と接続され、通信ネットワークＮ２を介して管理端末４００と接続される構成である。

【００２６】

まずホスト５００の構成を説明する。

【００２７】

ホスト５００は、通信インターフェース（図中「Ｉ／Ｆ」と略記）５１０、オペレーティングシステム（図中「ＯＳ」と略記）５２０及びアプリケーションプログラム５３０を備えている。ホスト５００は、通信インターフェース５１０からＳＡＮ等の通信ネットワークＮ１を介して、ストレージ装置１００にアクセスする。そしてアプリケーションプログラム５３０に基づいてホスト５００がファイルの操作等のデータ処理を行うと、このデータ処理に応じたコマンドがホスト５００から発行される。

【００２８】

なおコマンドとしては、データの書込みを要求するライトコマンド、データの読出しを要求するリードコマンド等がある。

【００２９】

次に管理端末４００の構成を説明する。

【００３０】

管理端末４００は、コンピュータ装置として構成されており、ＬＡＮ等の通信ネットワークＮ２を介してストレージ装置１００に接続される。管理端末４００は、ストレージ管理ソフトウェア４１０を備えている。ストレージ管理ソフトウェア４１０は、ストレージ装置１００の構成や設定状態等を管理し、ストレージ装置１００の各種情報を取得して表示させるためのプログラムである。ユーザは、ストレージ管理ソフトウェア４１０が提供する管理画面を操作することにより、暗号化に関する種々の設定を行うことができる。なお、管理画面の一例については後述する。

【００３１】

ストレージ装置１００の構成を説明する。

【００３２】

ストレージ装置１００は、記憶制御装置であり、ストレージ装置１００の動作を制御するコントローラ２００と、複数の記憶装置３３０Ａ，３３０Ｂを有する記憶装置搭載部３００とを備える。

【００３３】

コントローラ２００は、例えば、ホストインターフェース２１０と、バックエンドコントローラ２２０と、データ転送制御回路（図中「ＤＣＴＬ」と略記）２３０と、プロセッサ（図中「ＭＰＵ」と略記）２４０と、キャッシュメモリ２５０と、メモリ２６０と、ブリッジ２７０と、暗号化回路２８０と、ＬＡＮインターフェース２９０とを備えて構成される。

【００３４】

ホストインターフェース２１０は、ホスト５００との間の通信を制御する。ホスト５００から発行された各種コマンドやデータは、ホストインターフェース２１０によって受信される。記憶装置３３０Ａ，３３０Ｂから読み出されたデータやコマンドの処理完了を告げる通知は、ホストインターフェース２１０からホスト５００に送信される。

【００３５】

バックエンドコントローラ２２０は、各記憶装置３３０Ａ，３３０Ｂとの間の通信を制御する。バックエンドコントローラ２２０は、論理ブロックアドレス（ＬＢＡ）と記憶装置３３０Ａ，３３０Ｂの物理的なアドレスとの変換操作等を行う。

【００３６】

データ転送制御回路２３０は、コントローラ２００内のデータ転送を制御するための回路である。データ転送制御回路２３０は、ホストインターフェース２１０とキャッシュメモリ２５０との間のデータ転送や、バックエンドコントローラ２２０とキャッシュメモリ２５０との間のデータ転送を制御する。

【００３７】

プロセッサ２４０は、一つまたは複数のプロセッサコアを備えている。プロセッサ２４０は、メモリ２６０に記憶されたプログラムを読み込んで実行することにより、後述する各種の機能を実現する。

【００３８】

キャッシュメモリ２５０は、ホスト５００から受信したデータやホスト５００により読み出されたデータを記憶する。キャッシュメモリ２５０には、ライトデータやリードデータのユーザデータが記憶されるほかに、ストレージ装置１００内で行われる暗号化に関する各種の情報も記憶されている。

【００３９】

暗号化に関する各種の情報とは、暗号鍵２５１，暗号データアドレス管理テーブル２５２，暗号領域管理テーブル２５３，暗号化ポリシー管理テーブル２５４、暗号鍵管理テーブル２５５である。

【００４０】

そして、キャッシュメモリ２５０は、キャッシュメモリ２５０上に保存するユーザデー

タを記憶するための領域を備えており、図１においては、暗号領域Ａ２５８、暗号領域Ｂ２５７、平文領域２５６を明示的に示している。前記領域以外にも、ユーザデータの記憶量や単位に合わせて領域を確保する。

【００４１】

暗号鍵２５１は、ストレージ装置１００内で平文データを暗号化されたデータに暗号化し、又は、暗号化されたデータを平文データに復号化するために使用される。各種テーブル２５２～２５５については、別図と共に後述する。

【００４２】

メモリ２６０は、プログラムや制御情報を記憶するものである。メモリ２６０には、暗号化／復号化判定部２６１，暗号処理部２６２，復号処理部２６３，暗号鍵生成部２６４，記憶領域管理部２６５、暗号化ポリシー制御部２６６という各種の機能を実現するためのプログラムが記憶される。

【００４３】

なお、これら各機能を実現するためのプログラムまたは一部のプログラムは、ストレージ装置１００の起動時に、記憶装置３３０Ａ，３３０Ｂからメモリ２６０に転送させるようにしてもよい。

【００４４】

暗号化／復号化判定部２６１は、ホスト５００から受信したライトデータを暗号化するか否か、及び、ホスト５００から要求されたリードデータを復号化するか否かを判定するための機能である。

【００４５】

暗号処理部２６２は、暗号化／復号化判定部２６１で暗号化が決定されたデータについて、暗号化回路２８０を用いて、暗号処理を行う。

【００４６】

同様に、復号処理部２６３は、暗号化／復号化判定部２６１で復号化の決定されたデータについて、暗号化回路２８０を用いて復号処理を行う。

【００４７】

暗号鍵生成部２６４は、暗号処理や復号処理に使用するための暗号鍵を生成する。

【００４８】

記憶領域管理部２６５は、記憶装置３３０Ａ，３３０Ｂを生成したり、記憶装置３３０Ａ，３３０Ｂに暗号化の属性（暗号化記憶領域か非暗号化記憶領域かの区別）を設定したり、記憶装置３３０Ａ，３３０Ｂとホスト５００との接続関係等を設定するための機能である。これらの設定は、ユーザが管理端末４００を介して行う。

【００４９】

暗号化ポリシー制御部２６６は、ユーザの設定した暗号化ポリシーをストレージ装置１００に適用するためのデータ制御を行うための機能である。暗号化ポリシー制御部２６６は、ストレージ装置１００内部でのデータの暗号処理や復号処理、データのコピー処理や再暗号化処理等が設定されたポリシーを適用する際に必要となるデータ処理を行う。

【００５０】

ブリッジ２７０は、プロセッサ２４０とメモリ２６０とを接続する。また、プロセッサ２４０は、ブリッジ２７０を介してデータ転送制御回路２３０に接続される。

【００５１】

暗号化回路２８０は、平文データを暗号化されたデータに暗号化し、又は、暗号化されたデータを平文データに復号化するための回路である。暗号化回路２８０は、暗号処理部２６２により制御される。

【００５２】

暗号化回路２８０は、例えば、図１のように、データ転送制御回路２３０とバックエンドコントローラ２２０との間に設けることができる。これに代えて、例えば、データ転送制御回路２３０とホストインターフェース２１０との間に暗号化回路２８０を設ける構成、データ転送制御回路２３０内に暗号化回路２８０を設ける構成又はプロセッサ２４０内

に設ける構成、さらにはその他の構成をとってもよい。

【００５３】

ＬＡＮインターフェース２９０は、管理端末４００との通信を行うものである。

【００５４】

次に、記憶装置搭載部３００の構成を説明する。

【００５５】

記憶装置搭載部３００は、複数の記憶装置３３０Ａ，３３０Ｂを備えている。

【００５６】

記憶装置３３０Ａには、非暗号化記憶領域の属性が設定されており、平文データを記憶する。

【００５７】

他方の記憶装置３３０Ｂには、暗号化記憶領域の属性が設定されており、暗号データを記憶する。

【００５８】

なお、特に区別する場合を除いて、以下の説明では、記憶装置３３０Ａ，３３０Ｂを記憶装置３３０と表現する。

【００５９】

記憶装置３３０の構成を具体的に説明する。

【００６０】

まず、一つまたは複数の物理的な記憶装置３１０からＲＡＩＤグループ３２０が構成される。

【００６１】

以下、論理的な記憶装置３３０との混同を防止するために、物理的な記憶装置３１０をディスクドライブ３１０と表現し、論理的な記憶装置３３０をＬＵまたは論理ボリュームと表現する。また、暗号化記憶領域に設定されているＬＵ３３０を、図中では暗号化ＬＵと表現する場合がある。

【００６２】

なお、ディスクドライブ３１０は、例えば、ハードディスクドライブとして構成されるが、これに限らず半導体メモリ装置等から構成してもよい。

【００６３】

複数のディスクドライブ３１０がそれぞれ有する物理的な記憶領域をグループ化することにより、ＲＡＩＤグループ３２０が構築される。このＲＡＩＤグループ３２０の記憶領域に複数のＬＵ（論理ボリューム）３３０を設けることができる。

【００６４】

なお、上述のハードウェア構成は一例であって、本発明は上記構成に限定されない。すなわち、ホスト５００からのコマンドに応じてＬＵ３３０Ａ，３３０Ｂにデータを読み書きすることができ、管理端末４００からの指示に基づいて暗号化に関する設定情報を更新することができ、ストレージ装置１００の内部でデータを暗号化又は復号化することのできる構成を備えていればよい。

【００６５】

図２は、本実施の形態でのストレージ装置１００の運用方法における運用変更前後の概要図である。

【００６６】

本実施の形態のストレージ装置１００は、上述した論理ボリューム３３０のうち、ホスト５００からのデータを保存する論理ボリュームを正側の論理ボリュームとし、正側の論理ボリュームに保存されるデータのバックアップデータを保存する論理ボリュームを副側の論理ボリュームとして運用する。

【００６７】

また、ユーザはストレージ装置１００の運用中にストレージ装置１００に対して暗号化ポリシーを設定することで、平文データを保存して管理していた正側の論理ボリューム（

図中、平文正ＶＯＬと略記いう）を、ある時点で暗号化されたデータを保存して管理する正側の論理ボリューム（図中、暗号正ＶＯＬと略記）として運用する方法の変更を実施する。なお、平文正ボリューム及び暗号正ボリュームは、上述した論理ボリューム３３０から構成される。

【００６８】

図２において、上段に示す図はストレージ装置１００の運用を変更する前の複数の論理ボリューム内のデータ管理状態を示し、下段に示す図はストレージ装置１００の運用を変更した後の複数の論理ボリューム内のデータ管理状態を示している。

【００６９】

まずストレージ装置１００の運用を変更する前の場合では、平文正ボリュームが平文データを保存するように管理されている。この場合に、ストレージ装置１００は、平文正ボリュームのスナップショットを定期的に作成し、同時に平文データのバックアップを行い、バックアップデータを保存している。このバックアップデータも平文データの副側の論理ボリューム（図中、平文副ＶＯＬと略記）３に記憶され、管理されている。

【００７０】

ここで、ストレージ装置１００の運用を従来による方法で変更する。すなわち、平文データを暗号化して暗号正ボリューム内で管理する運用に変更する。この運用方法を変更した後に、スナップショットとして作成されるバックアップデータに関しても、暗号化されたデータとして副側の論理ボリューム（図中、暗号副ＶＯＬと略記）に保存される。従来による方法で運用を変更した以後は、図２の上段に示すように、ストレージ装置１００は暗号副ボリューム１及び暗号副ボリューム２を管理することとなる。

【００７１】

なお、暗号副ボリューム１及び暗号副ボリューム２は、暗号化されたデータを記憶するための論理ボリューム３３０であり、ボリューム数は図示したものに限られない。

【００７２】

ここで、ユーザがストレージ装置１００で運用中のデータを暗号化することによって、データ漏洩の防止を目的とした暗号化ポリシーで運用することができる。しかしながら、平文正ボリュームが暗号化される前に取得したバックアップデータに関しては、平文データのまま平文副ボリューム３内に記憶され続けている。したがって、ストレージ装置１００内のディスクドライブ３１０が盗まれる等の被害にあうおそれがあるため、データ漏洩の危険性が残ってしまう。

【００７３】

そこで図２に示す下段図では、平文正ボリュームを暗号化した時点で、ユーザが所望する暗号化ポリシーでストレージ装置１００を運用する場合を示す。ユーザが既存のバックアップデータを暗号化する設定を施していた場合には、ストレージ装置１００が平文正ボリュームを暗号化したことを契機に、平文副ボリュームを暗号副ボリューム３へと暗号化処理が行われたことを示している。

【００７４】

図３及び図４は、本実施の形態の別の運用形態を示した運用方法変更を示す概要図である。

【００７５】

図３及び４において、上段に示す図はストレージ装置１００の運用を変更する前の複数の論理ボリュームを示し、下段に示す図はストレージ装置１００の運用を変更した後の複数の論理ボリュームを示している。

【００７６】

ストレージ装置１００では、平文データを保存する平文正ボリューム１及び平文正ボリューム２が運用され、当該平文データのバックアップデータを保存する平文副ボリューム１～４が運用される形態を示している。また、ホスト５００からの更新命令に基づいて、平文副ボリューム１～４の実際のデータ（以下、これを実データという）の更新分に相当する差分データ（以下、これを実差分データという）を保存しておく平文プール領域（図

中、平文ＰＯＯＬと記載）がある。平文プール領域内には、実差分データを保存するボリューム（以下、これを平文差分ボリュームという）１～４があり、それぞれの差分ボリューム１～４はそれぞれの平文副ボリューム１～４と対応付けがされている。

【００７７】

なお、図３及び図４では、平文差分ボリューム１～４を平文差分ＶＯＬ１～４と記載する。

【００７８】

このような運用方法において、ストレージ装置１００の運用中に平文正ボリューム２を暗号化して暗号正ボリューム２として管理する運用方法に変更する。

【００７９】

この時、運用ケース１として、図３に示すように、これまで実差分データを保存していた平文プール領域とは別に暗号化されたデータのみを保存するための暗号プール領域（図中、暗号ＰＯＯＬと記載）を作成し、差分データを暗号化して保存するケースが挙げられる。この運用ケースによれば、ストレージ装置１００が平文プール領域と暗号プール領域とで保存するデータをそれぞれ平文データと暗号データに限定して保存する識別を実現する。

【００８０】

なお、図３及び図４では、差分データを暗号化して保存する論理ボリューム（以下、暗号差分ボリュームという）１、２を暗号差分ＶＯＬ１、２と記載する。

【００８１】

一方で、運用ケース２として、図４に示すように、平文プール領域内で平文差分ボリューム１，２を暗号化することによって、暗号差分ボリューム１，２として保存する。この時、平文プール領域内の平文差分ボリューム１，２と同じ領域にデータを書き戻しても、又は、平文プール領域内の別の領域を確保して暗号差分ボリューム１，２を作成して保存しても良い。本運用ケースによれば、前者での運用ケースを図４に示している。すなわち、同一のプール領域内に、暗号差分ボリューム１，２と平文差分ボリューム３，４とを保存する。この運用ケースによれば、暗号データと平文データとが同一プール領域内である混在プール領域（図中、混在ＰＯＯＬと記載）に混在して管理する方法を実現できる。

【００８２】

図５は、論理ボリュームの拡張等に伴う構成変更時に暗号化機能を運用するための方法を示す概要図である。

【００８３】

図５の第１段目に示す図５(Ａ)について説明する。ある暗号正ボリューム０に平文正ボリューム０を統合することで論理ボリュームを拡張する場合、統合前の暗号副ボリューム０と平文副ボリューム０とを統合して、統合後の暗号正ボリューム００に対応する暗号副ボリューム００を作成する。統合される側の論理ボリューム内に保存されるデータについては、消去する方式又はホスト５００等から継続して利用できる形態で暗号化して継続保存する方式でも良い。

【００８４】

図５の第２段に示す図５(Ｂ)について説明する。ある平文正ボリューム１に平文正ボリューム２を統合することで論理ボリュームを拡張する場合、統合前の平文副ボリューム１と平文副ボリューム２とを統合して、統合した平文副ボリューム１２として拡張する。

【００８５】

このとき、統合した平文副ボリューム１２は、平文副ボリューム１２のまま運用しても良いが、バックアップデータとしてテープドライブ等の可搬媒体に保存されるメディア盗難、紛失等による情報漏洩の危険性を考慮して、拡張後の平文副ボリューム１２を暗号化して暗号副ボリューム１２として運用しても良い。

【００８６】

暗号化のタイミングは暗号化ポリシーの設定に基づくが、平文副ボリューム１，２を統合した直後に暗号化を実施して暗号副ボリューム１２として運用する方法でも良いし、後

に平文副ボリューム１２を指定して、平文副ボリューム１２内に保存されるバックアップデータを暗号化して暗号副ボリューム１２として運用する方法でも良い。

【００８７】

つぎに、図５の第３段に示す図５(Ｃ)について説明する。ある暗号鍵ＫＥＹ１で暗号化された暗号正ボリューム３に暗号鍵ＫＥＹ２で暗号化された暗号正ボリューム４を統合する場合、統合前の暗号副ボリューム３，４を統合して、統合後の暗号副ボリューム３４に拡張する。暗号正ボリューム３４として統合する際に、暗号鍵ＫＥＹ２で暗号化されている暗号正ボリューム４は、暗号鍵ＫＥＹ２で一旦復号化した後、暗号鍵ＫＥＹ１で再び暗号化をする。

【００８８】

この時、暗号鍵ＫＥＹ１でバックアップされた暗号副ボリューム３に合わせて統合後の暗号副ボリューム３４も暗号鍵ＫＥＹ１で管理する暗号領域として運用する。

【００８９】

なお、統合される暗号副ボリューム３４内に保存されるデータについては、統合時に消去されることでも、暗号鍵ＫＥＹ１によって再暗号化されることで継続してデータを使用できる事でも良い。

【００９０】

つぎに、図５の第４段に示す図５(Ｄ)について説明する。ある暗号鍵ＫＥＹ３で暗号化された暗号正ボリューム５に暗号鍵ＫＥＹ４で暗号化された暗号正ボリューム６を統合する場合、統合前の暗号副ボリューム５，６を統合して、統合後の暗号副ボリューム５６に拡張する。なお暗号正ボリューム５６として統合する際に、暗号鍵ＫＥＹ３で暗号化した暗号正ボリューム５は、暗号鍵ＫＥＹ４で復号化した後、暗号鍵ＫＥＹ３で再暗号化をして統合する。

【００９１】

この時、暗号鍵ＫＥＹ４でバックアップされた暗号副ボリューム６に合わせて統合後の暗号副ボリューム５６も暗号鍵ＫＥＹ４で管理する暗号領域として運用する。

【００９２】

なお、統合後と暗号鍵の変わる暗号副ボリューム５に保存されるデータについては、統合時に消去されることでも、暗号鍵ＫＥＹ４によって再暗号化されることで継続してデータを使用できる事でも良い。また、図５(Ｃ)及び(Ｄ)で示した２つの運用ケースのように、複数の暗号鍵で管理されたボリュームを統合する場合には、暗号鍵の強度や、生成時間の新しさ等の基準でユーザが選択できる手段を提供してもよい。

【００９３】

上記の運用形態においては、初めの運用ではユーザには１つ以上の正ボリュームを含む暗号ボリュームや平文ボリュームが見えている。しかし、論理ボリュームを拡張する機能等の構成変更機能を使用して、１つの正ボリュームに１つ以上の他のボリュームを統合することによって、ユーザやホスト５００のＯＳ／アプリケーション等からは１つの論理ボリュームとして認識される事となる。

【００９４】

図６は、管理端末４００に表示される設定画面Ｇ１の例を示す説明図である。ユーザは、設定画面Ｇ１を呼び出すことにより、暗号機能に関する種々の設定を行う。即ち、暗号設定画面Ｇ１は、暗号領域管理テーブル２５３及び暗号鍵管理テーブル２５５をそれぞれ設定するためのユーザ・インターフェースとなっている。

【００９５】

設定画面Ｇ１には、例えば、複数の設定項目Ｇ１１～Ｇ１６、ＯＫボタンＧ１７及びキャンセルボタンＧ１８が含まれている。各設定項目Ｇ１１～Ｇ１６には、それぞれの名称が表示されており、ユーザは、その項目に設定する値を入力または選択する。

【００９６】

ＬＵＮ設定項目Ｇ１１は、暗号化対象のＬＵを指定するための項目である。設定項目Ｇ１１は、論理ボリューム３３０に付与される識別番号を選択することでＬＵＮを指定する

。

【００９７】

ホスト設定項目Ｇ１２は、ＬＵＮ設定項目Ｇ２１で指定した論理ボリューム３３０とホスト５００との対応関係性を設定する項目であり、ホスト５００を特定する。

【００９８】

暗号化単位設定項目Ｇ１３は、暗号化単位を実現する単位を指定する項目である。設定画面Ｇ１では、論理ボリューム単位を示すＬＵが設定されているが、ストレージ装置１００全体であったり、ＲＡＩＤグループ指定であったり、別の設定手段を設けても良い。

【００９９】

ＲＡＩＤグループ設定項目Ｇ１４は、暗号化対象のＲＡＩＤグループ指定項目であり、ＲＡＩＤグループの番号を指定することで特定する。ＬＵＮ設定項目Ｇ１１に指定したＬＵが所属するＲＡＩＤグループが設定されることとなる。

【０１００】

ストレージの暗号化機能設定項目Ｇ１５は、ストレージの暗号化機能の有効化／無効化を設定する項目である。設定画面Ｇ１では、「ＯＮ」が設定されているため暗号機能が有効とされているが、「ＯＦＦ」と設定されている場合には暗号化機能を使用しない。ただし、「ＯＮ」「ＯＦＦ」以外の判定基準となる値で設定しても良い。

【０１０１】

各設定項目Ｇ１１～Ｇ１６について設定を完了した場合、ユーザは、ＯＫボタンＧ１７を操作する。これにより、各設定項目Ｇ１１～Ｇ１６で設定された値が暗号領域管理テーブル２５３及び暗号鍵管理テーブル２５５に反映される。一方、入力した設定値を取り消したい場合、ユーザは、キャンセルボタンＧ１８を操作する。

【０１０２】

図７は、管理端末４００に表示される暗号ポリシー設定画面Ｇ２の例を示す説明図である。暗号ポリシー設定画面Ｇ２は、図６で説明をした設定画面Ｇ１に続いて表示される画面である。ユーザは、暗号ポリシー設定画面Ｇ２を呼び出すことにより、暗号化に関する種々の設定を行う。即ち、暗号ポリシー設定画面Ｇ２は、暗号領域管理テーブル２５３及び暗号化ポリシー管理テーブル２５４をそれぞれ設定するためのユーザ・インターフェースとなっている。

【０１０３】

設定画面Ｇ２には、例えば、複数の設定項目Ｇ２１～Ｇ２５、確定ボタンＧ１６及びキャンセルボタンＧ１７が含まれている。各設定項目Ｇ１１～Ｇ１５には、それぞれの名称が表示されており、ユーザは、その項目に設定する値を入力または選択する。

【０１０４】

ストレージの暗号化機能設定項目Ｇ２１は、暗号機能を備える設定対象のストレージ装置１００に対して、暗号化ポリシーを適用するか否かを設定するための項目である。

【０１０５】

ここで、暗号化ポリシーとは、暗号機能に関する属性の設定情報をいう。暗号機能に関する属性の設定情報とは、本実施の形態では、暗号機能を有効／無効にする設定、暗号機能が有効な場合の暗号領域の設定、暗号鍵の有無設定等、設定画面Ｇ１、Ｇ２及び後述する管理画面Ｇ３上でユーザが設定する事項が挙げられる。

【０１０６】

暗号化範囲設定項目Ｇ２２は、ストレージ装置１００内の暗号化するデータ範囲を設定するための項目である。暗号化ポリシー設定画面Ｇ２では、装置全体を示すＡＬＬを指定しているが、ＬＵＮ、ホスト５００のグループ番号等の範囲を識別するための値が予め設定されているものとする。

【０１０７】

その他、暗号化範囲設定項目Ｇ２２の設定では、例えばポート１等の、意味のある文字列に代えて設定することも可能であるし、各暗号範囲対象に予め設定されたニックネーム等を用いて設定してもよい。

【０１０８】
バックアップデータ暗号設定項目Ｇ２３は、ユーザが暗号機能を有効化した場合にホストからの入出力データだけでなく、対象の論理ボリュームに関連づけられている既存のバックアップデータについても暗号化する対象とするかを設定するための項目である。暗号化ポリシー設定画面Ｇ２では、バックアップデータの暗号化を有効にする「ＯＮ」が設定されているが、「ＯＦＦ」が設定されている場合には、当該バックアップデータの暗号化を行わないことを示す。また、数値等による設定識別手段を提供しても良い。暗号化の対象としては、ストレージ装置１００内で取得されたスナップショットを初めとするバックアップデータである。
【０１０９】
差分データ暗号設定項目Ｇ２４は、差分データの暗号化に関わる設定を行うための項目である。ここで差分データとは、時系列的にバックアップを取る場合の前回バックアップ分と更新分との差分データ、スナップショットの差分の実データ又はジャーナルデータのことをいう。
【０１１０】
また、それ以外にストレージ装置１００を管理する上で必要な差分管理をする機能についても適用する。
【０１１１】
既存暗号データRekey設定項目Ｇ２５は、ストレージ装置１００に既に暗号データとして格納しているデータを再暗号化する記憶領域として使用するか否かを設定するための項目である。例えば、既存暗号データRekey設定項目Ｇ２５を「ＯＮ」に設定すると、暗号データとして格納しているデータを再び暗号化する記憶領域として選択することになる。
【０１１２】
暗号化記憶領域設定項目Ｇ２６は、Ｇ１１で設定された論理ボリューム３３０の記憶領域を暗号化させて使用するか否かを設定するための項目である。例えば、暗号化記憶領域設定項目Ｇ２６を「ＯＮ」に設定すると、Ｇ１１で設定された論理ボリューム３３０は暗号化記憶領域として使用される。暗号化記憶領域設定項目Ｇ２６を「ＯＦＦ」に設定すると、Ｇ１１で設定された論理ボリューム３３０は非暗号化記憶領域として使用される。設定値に関しては「ＯＮ」／「ＯＦＦ」でなくても数値等判定できる手段であればよい。
【０１１３】
各設定項目Ｇ２１～Ｇ２６について設定を完了した場合、ユーザは、確定ボタンＧ２７を操作する。これにより、各設定項目Ｇ２１～Ｇ２６で設定された値が暗号領域管理テーブル２５３及び暗号化ポリシー管理テーブル２５４に反映される。一方、入力した設定値を取り消したい場合、ユーザは、キャンセルボタンＧ２８を操作する。
【０１１４】
なお、上述した設定項目を増減させてもよい。即ち、ストレージ装置１００に設定すべき条件に応じて、図７に示す項目以外の項目を追加することもできるし、図７に示す項目から一部を取り除くこともできる。また、グラフィカルユーザインターフェースに代えて、例えば、コマンドラインから設定値を入力するユーザ・インターフェース等の他のユーザ・インターフェースを採用してもよい。
【０１１５】
図８は、暗号鍵管理画面２５１の例を示す説明図である。暗号鍵管理画面Ｇ３は、図７で説明をした設定画面Ｇ２に続いて表示される画面である。ユーザは、暗号鍵設定画面Ｇ３を呼び出すことにより、暗号鍵に関する種々の設定を行う。即ち、暗号鍵設定画面Ｇ３は、暗号鍵２５１及び暗号鍵管理テーブル２５５をそれぞれ設定するためのユーザ・インターフェースとなっている。
【０１１６】
設定画面Ｇ３には、例えば、複数の設定項目Ｇ３１～Ｇ３４と、ボタンＧ３５，Ｇ３６とが含まれている。各設定項目には、それぞれの名称が表示されており、ユーザは、その項目に設定する値を入力または選択する。

【０１１７】
ストレージのＬＵ領域指定項目Ｇ３１は、設定対象のストレージ装置１００のＬＵＮを特定するための情報を入力するための項目である。
【０１１８】
ＲＡＩＤグループ指定項目Ｇ３２は、設定対象のストレージ装置１００のＲＡＩＤグループを特定するための情報を入力するための項目である。
【０１１９】
ストレージのＬＵ領域指定項目Ｇ３１及びＲＡＩＤグループ指定項目Ｇ３２には、一般的に対応する数値が指定されるが、その他の値を入力して適切な形で解釈することで領域の特定を行えることでも良い。
【０１２０】
鍵種別指定項目Ｇ３３では、各ＬＵＮに割り当てる鍵の種別を指定するための項目である。鍵の割当てポリシーに従って、割当て単位がＬＵ毎であれば、各ＬＵＮに異なる鍵を設定しても良い。
【０１２１】
暗号化単位指定項目Ｇ３４では、暗号鍵の適用領域となる単位を指定するための項目である。設定画面Ｇ３では、ＲＡＩＤグループを指定しているが、ストレージ装置１００全体、ＬＵ単位又は他の単位であっても構わない。暗号化単位指定項目Ｇ３４では、設定を許可する単位にあわせた設定手段を提供する。
【０１２２】
図９は、キャッシュメモリ２５０に格納される暗号データアドレス管理テーブル２５２の例を示す説明図である。
【０１２３】
暗号データアドレス管理テーブル２５２には、ストレージ装置１００内で暗号化されたデータの格納先を管理するための情報が記憶されている。暗号データアドレス管理テーブル２５２は、例えば、「ＬＵＮ」フィールド２５２１、「ＲＡＩＤグループ」フィールド２５２２、「スタートＬＢＡ」フィールド２５２３及び「ＬＥＮ」フィールド２５２４から構成される。
【０１２４】
「ＬＵＮ」フィールド２５２１には、暗号化されたデータを書込む先の論理ボリューム３３０を特定する情報が格納される。すなわち、「ＬＵＮ」フィールド２５２１には、暗号化された論理ボリュームのボリューム番号が格納される。
【０１２５】
「ＲＡＩＤグループ」フィールド２５２２には、暗号化されたデータの書込み先である論理ボリューム３３０が所属するＲＡＩＤグループ３２０のグループ番号を特定する情報が格納される。
【０１２６】
「スタートＬＢＡ」フィールド２５２３には、暗号化されたデータの書き込まれた先頭アドレスを示す情報が格納され、具体的にはＬＢＡ（Logical Block Address）の値として設定される。
【０１２７】
「ＬＥＮ」フィールド２５２４には、書き込まれた暗号化されたデータのサイズを示す情報が格納される。
【０１２８】
図１０は、キャッシュメモリ２５０に格納される暗号領域管理テーブル２５３の例を示す説明図である。
【０１２９】
暗号領域管理テーブル２５３は、ＩＤ番号を付与されたストレージ装置１００上の領域に関して、暗号化の要否、暗号化する場合に使用する鍵の指定及びＩＤの表す領域を暗号化することで併せて暗号処理の必要性が生じる可能性のある関連領域を対応づけて管理す

るためのテーブルである。
【０１３０】
暗号領域管理テーブル２５３は、ストレージ装置１００内の領域を一意に管理するための「ＩＤ」フィールド２５３１、ＩＤの表す領域が所属する「ＲＡＩＤグループ」フィールド２５３２、「ＬＵＮ」フィールド２５３３、暗号領域の暗号化に使用する「暗号鍵」フィールド２５３４、ＩＤの表す領域を暗号化するか否かを指定する「暗号属性」フィールド２５３５及び暗号領域に関わるバックアップ先及びリストア先、プライマリデータと関連性のある論理ボリュームを示す「関連領域」フィールド２５３６から構成されている。
【０１３１】
なお、図１０の「暗号属性」フィールド２５３５において、「１」は暗号化された領域を示し、「０」は暗号化されていない領域を示している。
【０１３２】
図１１は、キャッシュメモリ２５０に格納される暗号化ポリシー管理テーブル２５４の例を示す説明図である。
【０１３３】
暗号化ポリシー管理テーブル２５４は、ストレージ装置１００内における暗号化ポリシーの管理状態を示すテーブルである。
【０１３４】
暗号化ポリシー管理テーブル２５４は、暗号機能に関わるさまざまな項目や機能の状態を指定するための「暗号機能項目」フィールド２５４１、前記暗号機能項目の更なる詳細情報を指定するための「詳細項目」フィールド２５４２、前記暗号機能項目２５４１及び詳細項目２５４２に対する暗号等に関わる設定値を指定するための「設定値」フィールド２５４３から構成される。
【０１３５】
「暗号機能項目」フィールド２５４１では、暗号機能の有効化無効化等の設定項目から、暗号化の単位や暗号範囲、再暗号化を示すＲｅｋｅｙ等に関わる設定を行う。
【０１３６】
「詳細項目」フィールド２５４２は、「暗号機能項目」フィールド２５４１での暗号範囲をさらに詳細に設定するためのフィールドである。具体的には、暗号範囲の詳細項目としては、プライマリデータだけでなく、バックアップデータ、差分データおよびリモートコピーデータに対して暗号化できるように設定されている。
【０１３７】
これにより、暗号ポリシーを有効化した時に、暗号化対象領域に対して、暗号化を設定した以降におけるホスト５００等からのデータだけでなく、暗号化対象領域に関連する既存の平文バックアップデータ、差分データ等に関してもストレージ装置１００内で連動して暗号化処理を実施することができる。
【０１３８】
このようなユーザがストレージ装置１００を使用する上での暗号化に関わるポリシーを設定できる手段を提供できればよく、本実施の形態におけるテーブルに記載していないが、例えば、暗号アルゴリズム等の暗号機能を「暗号機能項目」フィールド２５４１に追加してもよく、本実施の形態で示すテーブルの形式に限定しない。
【０１３９】
図１２は、キャッシュメモリ２５０に格納される暗号鍵管理テーブル２５５の例を示す説明図である。
【０１４０】
暗号鍵管理テーブル２５５は、論理ボリューム３３０に暗号鍵を設けて暗号化処理を実施するか否かを管理するためのテーブルである。
【０１４１】
暗号鍵管理テーブル２５５は、「鍵種別」フィールド２５５１、「ＲＡＩＤグループ」

フィールド２５５２、「ＬＵＮ」フィールド２５５３及び「鍵生成年月日時刻」フィールド２５５４から構成される。

【０１４２】

「鍵種別」フィールド２５５１には、暗号鍵、あるいは暗号鍵を特定する情報が格納される。

【０１４３】

「ＲＡＩＤグループ」フィールド２５５２には、鍵種別２５５１で指定した暗号鍵を使用して暗号化対象とする領域となるＲＡＩＤグループのグループ番号が格納される。

【０１４４】

「ＬＵＮ」フィールド２５５３には、「ＲＡＩＤグループ」フィールド２５５２内で指定したＲＡＩＤグループ内の論理ボリューム３３０を特定するための論理ボリューム番号が格納される。

【０１４５】

「鍵生成年月日時刻」フィールド２５５４は、「鍵種別」フィールド２５５１内で指定した暗号鍵が生成された年月日及び秒まで表示された時刻の情報が格納される。

【０１４６】

例えば、図１２においては、「key1」はＲＡＩＤグループ「０１」のＬＵＮ「００」からＬＵＮ「０２」全体に適用される。また「key1」の鍵生成年月日時刻は、２００７／０１／１０／１３：５８：２０という情報が格納されていることから、２００７年１月１０日１３時５８分２０秒に暗号鍵が生成されたことを示す。なお、フォーマットや時刻の粒度等はユーザの運用に併せて変更可能として良い。

【０１４７】

なお、他のテーブルについても同様であるが、本発明の目的を達成できるのであれば、各テーブルの構成は図示するもの以外の構成でもよい。

【０１４８】

図１３は、管理端末４００、ホスト５００等から暗号化ポリシーの適用を指示されたときのストレージ装置１００の処理を表すフローチャートを示す。暗号化ポリシー適用処理は、ストレージ装置１００のプロセッサ２４０が暗号化ポリシー制御部２６６、暗号化／復号化判定部２６１、暗号処理部２６２及び復号処理部２６３に基づいて実行する。

【０１４９】

以降で説明する各フローチャートは、処理の概要を示すもので、実際のコンピュータプログラムとは相違する場合がある。なお、以下の説明では、ステップを「Ｓ」と略記する。

【０１５０】

まず、ストレージ装置１００のプロセッサ２４０は、管理端末４００等から暗号化に関わる設定を実施された暗号設定処理を受信すると（Ｓ１０）、暗号化ポリシー適用処理を開始する。

【０１５１】

次に、プロセッサ２４０は、受信した暗号ポリシーがストレージ装置１００に適用可能か暗号化ポリシーのチェックを実施する（Ｓ１１）。受信した暗号ポリシーとは、上述した設定画面Ｇ１、Ｇ２及び管理画面Ｇ３によってユーザが設定した暗号ポリシーである。

【０１５２】

そして、プロセッサ２４０は、受信した暗号化ポリシー設定情報で暗号化ポリシー管理テーブル２５３を書き換える（Ｓ１２）。例えば、受信した暗号ポリシーがストレージ装置１０に適用可能な場合には、暗号化ポリシー管理テーブル２５４の暗号機能を無効から有効に更新する。

【０１５３】

プロセッサ２４０は、ストレージ装置１００のコントローラ２００上で暗号化ポリシー設定情報を読み出して、暗号化判定処理を実施する（Ｓ１３）。暗号化判定処理については、後述する。

【０１５４】
プロセッサ２４０は、ステップＳ１３の暗号化判定処理の結果を受けて、暗号化処理が必要か否かを判定する（Ｓ１４）。
【０１５５】
ここで暗号化処理とは、プライマリデータ及びプライマリデータに関連するデータを暗号化する処理をいう。
【０１５６】
そしてプロセッサ２４０は、暗号化処理が必要であると判定した場合は（Ｓ１４：ＹＥＳ）、暗号化適用処理を行う（Ｓ１５）。プロセッサ２４０は、暗号化処理が必要な論理ボリューム３３０に対して暗号化処理を実行する。必要な論理ボリューム３３０とは、暗号化処理が必要な平文正ボリューム、平文正ボリュームと関連性のある平文副ボリュームをいう。暗号化処理については、後述する。
【０１５７】
一方、プロセッサ２４０は、暗号化処理が不要であると判定した場合には（Ｓ１４：ＮＯ）、ステップＳ１６に進む。
【０１５８】
最後に、プロセッサ２４０は、要求処理を全部完了したかチェックし（Ｓ１６）、判定の結果まだ暗号化ポリシーにもとづく暗号化関連処理が完了していないと判定した場合には（Ｓ１６：ＮＯ）、ステップＳ１３に戻り、暗号化判定処理を再び実施する（Ｓ１３）。
【０１５９】
例えば、暗号化処理を設定した全ての論理ボリューム３３０に対して暗号化処理が終了していない場合、プライマリデータの暗号化処理が終了していない場合、プライマリデータに関連するデータの暗号化処理が終了していない場合、又は、暗号鍵の再設定が終了していない場合等には、ステップＳ１３に戻る。
【０１６０】
一方、プロセッサ２４０は、全ての要求処理が完了したと判断した場合には（Ｓ１６：ＹＥＳ）、暗号化ポリシー適用処理を終了する（Ｓ１７）。
【０１６１】
上述したステップのうち、ステップＳ１３では、プロセッサ２４０が暗号化／復号化判定部２６１に基づいて実行し、ステップＳ１５では、プロセッサ２４０が暗号処理部２６２及び復号処理部２６３に基づいて実行する。
【０１６２】
図１４は、図１３における暗号化判定処理（Ｓ１３）を詳細化した処理を表すフローチャートを示す。暗号化判定処理は、ストレージ装置１００のプロセッサ２４０が暗号化／復号化判定部２６１、暗号化ポリシー制御部２６６及び記憶領域管理部２６５に基づいて実行する。
【０１６３】
まず、ストレージ装置１００のプロセッサ２４０は、コントローラ２００上で暗号ポリシー管理テーブルを読込むと（Ｓ２０）。暗号化判定処理を開始する。
【０１６４】
次に、プロセッサ２４０は、暗号化ポリシー管理テーブル２５４から暗号機能項目を一項目取得する（Ｓ２１）。
【０１６５】
そして、プロセッサ２４０は、暗号化ポリシー管理テーブル２５４から取得した暗号機能項目に対応する詳細項目及び設定値を取得する（Ｓ２２）。
【０１６６】
ここで、プロセッサ２４０は、暗号化ポリシー管理テーブル２５４を参照し、取得した設定値に暗号化の要求があるか否かを判定する（Ｓ２３）。
【０１６７】

そして、プロセッサ２４０は、暗号化の要求がないと判定した場合には（Ｓ２３：ＮＯ）、ステップＳ２６に進む。

【０１６８】

一方、プロセッサ２４０は、暗号化の要求があると判定した場合には（Ｓ２３：ＹＥＳ）、暗号化対象情報取得処理を行う（Ｓ２４）。暗号化対象情報取得処理については、後述する。

【０１６９】

その後、プロセッサ２４０は、暗号化フラグをＯＮに設定する（Ｓ２５）。すなわち、暗号領域管理テーブル２５３の「暗号属性」フィールド２５３５の値を「１」に設定する。

【０１７０】

次に、プロセッサ２４０は、暗号化ポリシー管理テーブル２５４にある暗号機能項目の最終項目まで暗号化判定処理を実行したか否かを判定する（Ｓ２６）。

【０１７１】

そして、プロセッサ２４０は、暗号機能項目の最終項目まで暗号化判定処理を実行していないと判定した場合には（Ｓ２６：ＮＯ）、ステップＳ２１に戻り、引き続き暗号化判定処理を行う。

【０１７２】

一方プロセッサ２４０は、暗号機能項目の最終項目まで暗号化判定処理を実行したと判定した場合には（Ｓ２６：ＹＥＳ）、暗号化判定処理を終了する（Ｓ２７）。そしてプロセッサ２４０は、暗号化判定処理の結果に基づいて、図１３に示すステップＳ１４を実行することとなる。

【０１７３】

上述したステップのうち、ステップＳ２０～Ｓ２２では、プロセッサ２４０が暗号化ポリシー制御部２６６に基づいて実行し、ステップＳ２４では、プロセッサ２４０が記憶領域管理部２６５に基づいて実行する。

【０１７４】

図１５は、図１４における暗号化対象情報取得処理（Ｓ２４）を詳細化した処理を表すフローチャートを示す。暗号化対象情報取得処理は、ストレージ装置１００のプロセッサ２４０が記憶領域管理部２６５及び暗号化ポリシー制御部２６６に基づいて実行する。

【０１７５】

まず、ストレージ装置１００のプロセッサ２４０は、コントローラ２００上で暗号領域管理テーブル２５３を読み込む（Ｓ３０）。引き続き、プロセッサ２４０は、暗号データアドレス管理テーブル２５２を読み込む（Ｓ３１）。

【０１７６】

プロセッサ２４０は、暗号領域管理テーブル２５３と暗号データアドレス管理テーブル２５２とを読み込むことで暗号化されたデータの保存先を決定する。

【０１７７】

暗号化されたデータの保存先としては、暗号領域管理テーブル２５３を読み込んで、予め暗号化された記憶領域に暗号化されたデータを保存する場合と、暗号データアドレス管理テーブル２５２を読み込んで、暗号化されたデータを暗号化される前に保存していた記憶領域内に戻して保存する場合とがある。暗号化されたデータを同じ記憶領域内に戻して保存する場合において、コントローラ２００が暗号化されたデータと平文データとを同じ記憶領域内でのアドレスで管理するため、同じ記憶領域内に暗号化されたデータと平文データとを混在させて管理することとなる。

【０１７８】

次に、プロセッサ２４０は、暗号鍵管理テーブル２５５を読み込む（Ｓ３２）。そして、プロセッサ２４０は、読み込んだ各種テーブルの情報を基に暗号化対象情報を取得する（Ｓ３３）。

【０１７９】

例えば、図１１に示す暗号化ポリシー管理テーブル２５４の暗号単位に「装置」と設定されている場合には、暗号領域管理テーブル２５３を参照し、ＲＡＩＤグループ「０１」から「０３」の記憶領域が暗号化対象情報ということになる。

【０１８０】

そしてプロセッサ２４０は、暗号領域管理テーブル２５３の「関連領域」フィールド２５３６を参照し、暗号化対象情報である記憶領域に関連して暗号化する必要がある記憶領域があるか否か、暗号化対象情報に関連する記憶領域の有無を判定する（Ｓ３４）。

【０１８１】

判定の結果、プロセッサ２４０は、関連する記憶領域があると判定した場合には（Ｓ３４：ＹＥＳ）関連する記憶領域の情報を取得する（Ｓ３５）。関連する記憶領域についての情報は、暗号化対象情報を取得した場合と同様に、各種テーブル２５２，２５３，２５５から情報を取得できる。

【０１８２】

例えば、図１０の暗号領域管理テーブル２５３の「ＩＤ」フィールド２５３１の値が「０２」である記憶領域を参照する。そうすると、「０２」である記憶領域と関連する記憶領域として、「ＩＤ００－ＳＶＯＬ」が設定されていることがわかる。「ＩＤ００－ＳＶＯＬ」は、「ＩＤ」フィールド２５３１の値が「００」の記憶領域が副ボリュームであることを示している。なお、本設定例に限定しないが、記憶領域間の関連性が情報として取得できればよい。

【０１８３】

一方、Ｓ３４における判定の結果、プロセッサ２４０は、関連する記憶領域が無いと判定した場合には（Ｓ３４：ＮＯ）、ステップＳ３６に進む。

【０１８４】

プロセッサ２４０は、ステップＳ３０からＳ３２において読み込んだテーブル２５２，２５３，２５５から暗号処理の詳細設定を取得して同設定に基づいた暗号処理を行うための処理内容を取得する（Ｓ３６）。

【０１８５】

同様に、プロセッサ２４０は、読み込んだテーブル２５２，２５３，２５５から暗号鍵情報を取得すると（Ｓ３７）、暗号化対象情報取得処理を終了する（Ｓ３８）。そしてプロセッサ２４０は、暗号化判定処理の結果に基づいて、図１４に示すステップＳ２５を実行することとなる。

【０１８６】

上述したステップのうち、ステップＳ３２及びＳ３４～Ｓ３７では、プロセッサ２４０が暗号化ポリシー制御部２６６に基づいて実行する。

【０１８７】

図１６は、図１３の暗号化適用処理（Ｓ１５）を詳細化した処理を表すフローチャートを示す。暗号化判定処理は、ストレージ装置１００のプロセッサ２４０が暗号化ポリシー制御部２６６、暗号処理部２６２及び復号処理部２６３に基づいて実行する。

【０１８８】

まず、プロセッサ２４０は、暗号化適用処理を実行するまでの処理で取得した情報を基に、暗号化処理の対象となる記憶領域に保存されるデータを読み出す（Ｓ４０）。

【０１８９】

次に、プロセッサ２４０は、暗号対象領域データの暗号化について、設定された暗号鍵で暗号処理を行う（Ｓ４１）。プロセッサ２４０は、暗号化処理の対象である記憶領域を暗号領域にし、記憶領域に保存される平文データを暗号化する。

【０１９０】

そして、プロセッサ２４０は、暗号化されたデータを暗号領域に書き戻す（Ｓ４２）。

【０１９１】

続いて、プロセッサ２４０は、暗号領域の関連領域があるかないかを判定する（Ｓ４３）。プロセッサ２４０は、関連領域が存在すると判定した場合には（Ｓ４３：ＹＥＳ）、

図１５の暗号化対象情報取得処理の結果に基づき、関連する記憶領域からデータを読み出す（Ｓ４４）。

【０１９２】

そしてプロセッサ２４０は、設定された暗号鍵を使用して関連する記憶領域に保存されるデータの暗号処理を行い（Ｓ４５）、暗号化したデータを暗号領域へ書き戻す（Ｓ４６）。

【０１９３】

最後に、プロセッサ２４０は、完了通知を管理端末４００に報告し（Ｓ４７）、暗号化適用処理を終了する（Ｓ４８）。

【０１９４】

なお、Ｓ４３において、プロセッサ２４０は、関連領域が存在しないと判定した場合には（Ｓ４３：ＮＯ）、そのまま完了通知を管理端末４００に報告し（Ｓ４７）、暗号化適用処理を終了する（Ｓ４８）。

【０１９５】

上述したステップのうち、ステップＳ４１及びＳ４５では、プロセッサ２４０が暗号処理部２６２及び復号処理部２６３に基づいて実行する。

【０１９６】

本発明は、上述した実施の形態に限定されない。当業者であれば、本発明の範囲内で、種々の追加や変更等を行うことができる。

【０１９７】

本実施の形態では、データを暗号化するための情報である暗号機能に関する属性の設定情報を管理する設定情報管理部をキャッシュメモリ２５０に設け、暗号機能に関する属性の設定情報に基づいて、ホスト装置からのデータと記憶装置に記憶されるデータとの暗号化を行う暗号化実行部をメモリ２６０に設けたが、設定情報管理部及び暗号化実行部は個別のハードウェア構成としてもよい。

【０１９８】

また、前記暗号機能に関する属性の設定情報に基づいて、ホスト装置からのデータ又は前記記憶装置に記憶されるデータの暗号化を行うか否かの判定を行う暗号化判定部をメモリ２６０に設けたが、上述と同様に暗号化判定部は個別のハードウェア構成としてもよい。

【産業上の利用可能性】

【０１９９】

本発明は、１又は複数の記憶制御装置を有するストレージシステムや、その他の形態のストレージシステムに広く適用することができる。

【図面の簡単な説明】

【０２００】

【図１】本実施の形態におけるストレージシステムの全体構成を示す説明図である。

【図２】本実施の形態におけるストレージ装置内でのバックアップデータの暗号化運用例を示す概要説明図である。

【図３】本実施の形態におけるストレージ装置内での更新差分データの暗号化運用例を示す概要説明図である。

【図４】本実施の形態におけるストレージ装置内での更新差分データの暗号化運用例を示す概要説明図である。

【図５】本実施の形態におけるストレージ装置内の記憶領域の構成を変更する時のデータの暗号化運用例を示す概要説明図である。

【図６】本実施の形態における暗号処理の設定画面を示す説明図である。

【図７】本実施の形態における暗号化ポリシー設定画面を示す説明図である。

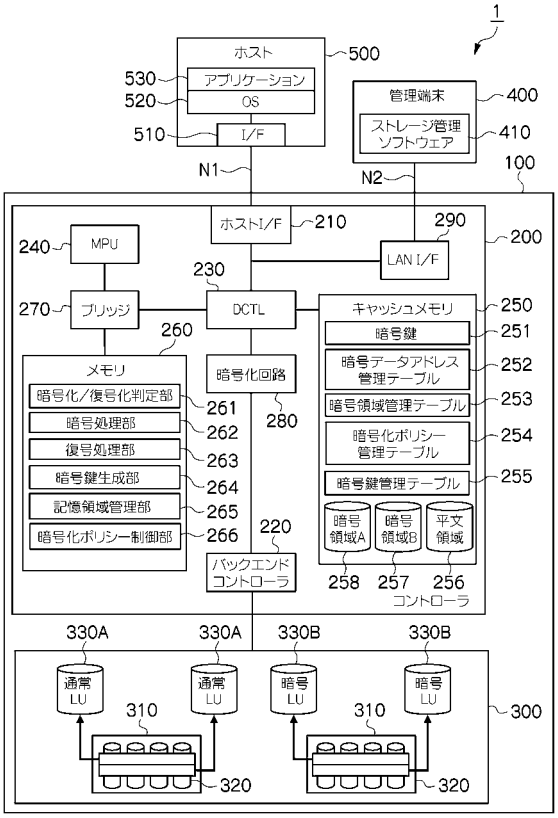
【図８】本実施の形態における暗号鍵管理画面を示す説明図である。

【図９】本実施の形態における暗号データアドレス管理テーブルを示す図表である。

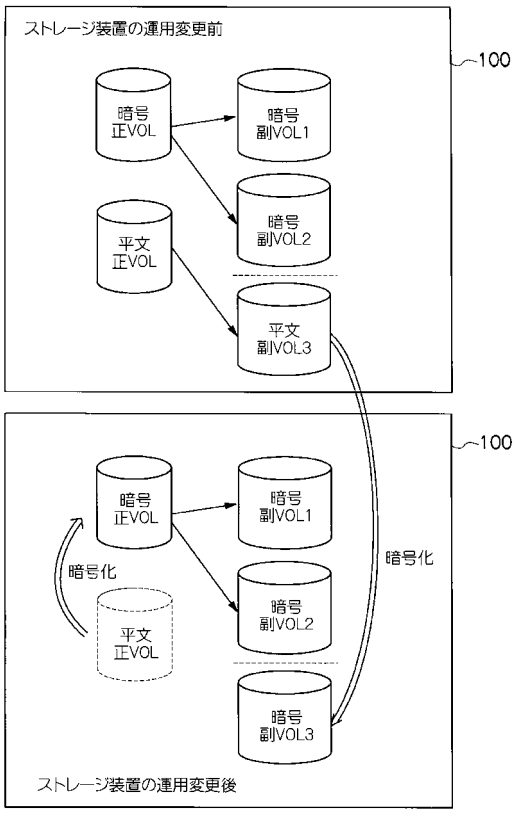
【図１０】本実施の形態における暗号領域管理テーブルを示す図表である。

【図１１】本実施の形態における暗号化ポリシー管理テーブルを示す図表である。
【図１２】本実施の形態における暗号鍵管理テーブルを示す図表である。
【図１３】本実施の形態における暗号化ポリシー適用処理を示すフローチャートである。
【図１４】本実施の形態における暗号化判定処理を示すフローチャートである。
【図１５】本実施の形態における暗号化対象情報取得処理を示すフローチャートである。
【図１６】本実施の形態における暗号化適用処理を示すフローチャートである。
【符号の説明】
【０２０１】
ＣＮ…通信ネットワーク、１００…ストレージ装置、２００…コントローラ、２１０…ホストインターフェース、２２０…バックエンドコントローラ、２３０…データ転送制御回路、２４０…プロセッサ、２５０…キャッシュメモリ、２５１…暗号鍵、２５２…暗号データアドレス管理テーブル、２５３…暗号領域管理テーブル、２５４…暗号化ポリシー管理テーブル、２５５…暗号鍵管理テーブル、２６０…メモリ、２６１…暗号化／復号化判定部、２６２…暗号処理部、２６３…復号処理部、２６４…暗号鍵生成部、２６５…記憶領域管理部、２６６…暗号化ポリシー制御部、２７０…ブリッジ、２８０…暗号化回路、２９０…ＬＡＮインターフェース、３００…記憶装置搭載部、３１０…ディスクドライブ、３２０…ＲＡＩＤグループ、３３０，３３０Ａ，３３０Ｂ…論理ボリューム（ＬＵ）、４００…管理端末、４１０…ストレージ管理ソフトウェア、５００…ホスト、５１０…インターフェース、５２０…ＯＳ、５３０…アプリケーションプログラム。

【図１】
図1

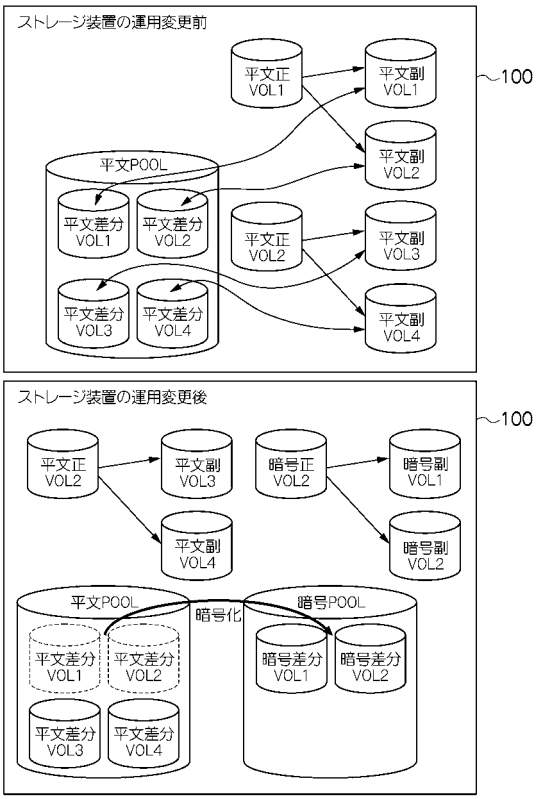


【図２】
図2



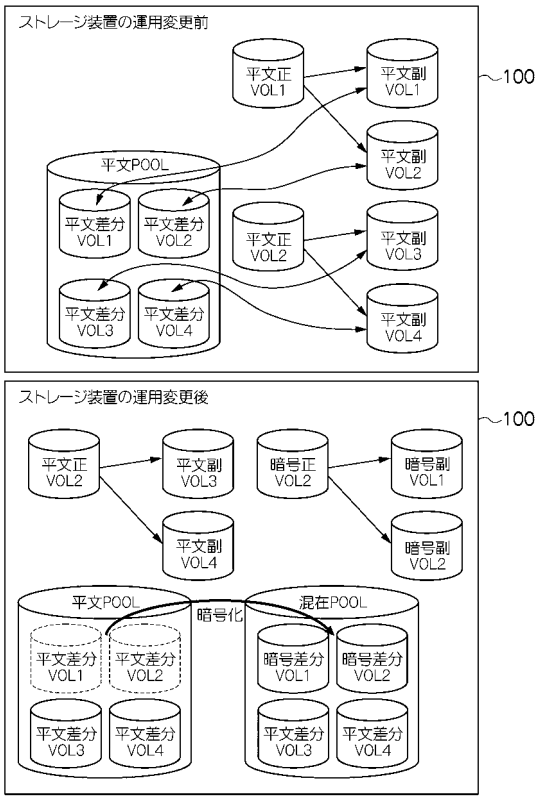
【図３】

図3



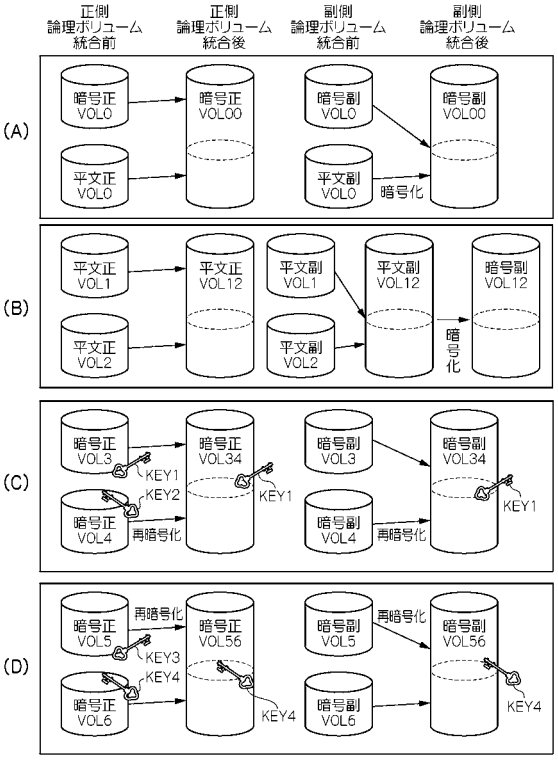
【図４】

図4



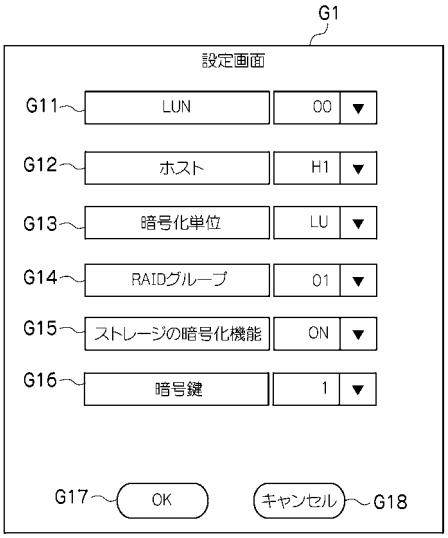
【図５】

図5

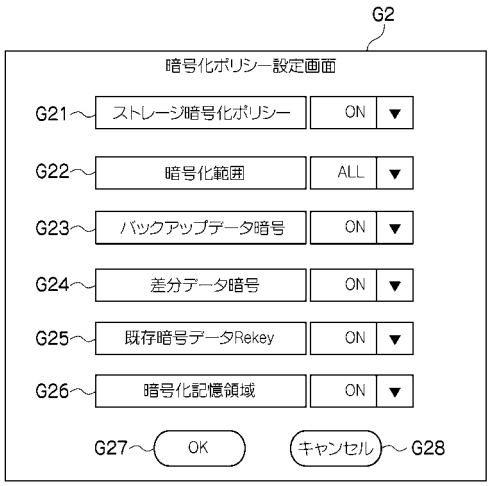


【図６】

図6



【図７】
図7



【図８】
図8

G3

暗号鍵管理画面

G31 LUN	G32 RAIDグループ	G33 鍵種別	G34 暗号化単位
00	01	key1	RAIDグループ
01	01	key1	RAIDグループ
02	01	key1	RAIDグループ
03	01	key1	RAIDグループ
00	02	key2	RAIDグループ
01	02	key2	RAIDグループ

G35 OK　キャンセル G36

【図９】
図9

252

暗号データアドレス管理テーブル

2521 LUN	2522 RAIDグループ	2523 スタートLBA	2524 LEN
00	01	512B	k
00	01	1024B	l
00	02	512B	m
00	03	2048B	n

【図１０】
図10

253

暗号領域管理テーブル

2531 ID	2532 RAIDグループ	2533 LUN	2534 暗号鍵	2535 暗号属性	2536 関連領域
00	01	00	key1	1	–
01	01	01	key1	1	–
02	02	00	key1	1	ID00-SVOL
03	02	01	key2	1	ID00-SVOL
04	03	00	–	0	ID01-VVOL

【図１１】
図11

254

暗号化ポリシー管理テーブル

2541 暗号機能項目	2542 詳細項目	2543 設定値
暗号機能		有効
暗号単位		装置
暗号範囲	プライマリデータ	暗号化
	バックアップデータ	暗号化
	差分データ	暗号化
	リモートコピーデータ	平文
Rekey		2008/01/10

【図１２】

図12

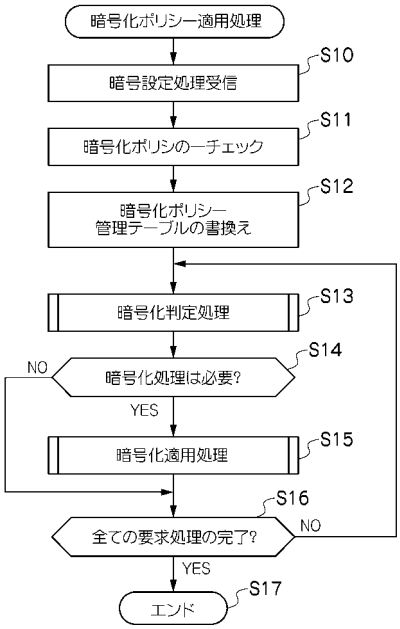
255

暗号鍵管理テーブル

2551	2552	2553	2554
鍵種別	RAIDグループ	LUN	鍵生成年月日時刻
key1	01	00	2007/01/10/13:58:20
	01	01	2007/01/10/13:58:20
	01	02	2007/01/10/13:58:20
key2	02	00	2007/01/15/09:00:12
key3	03	00	2007/01/18/12:15:13
key4	04	00	2007/01/18/12:18:14

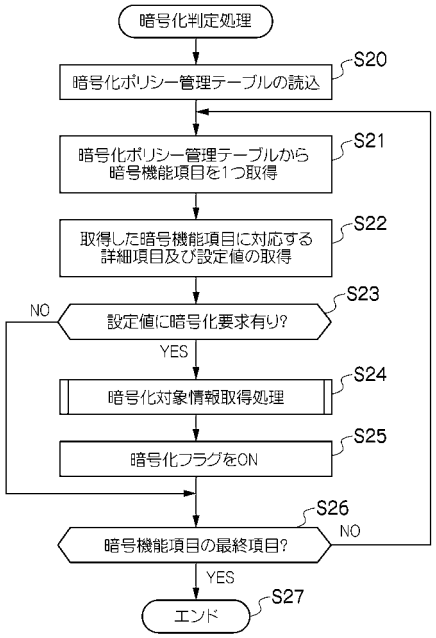
【図１３】

図13



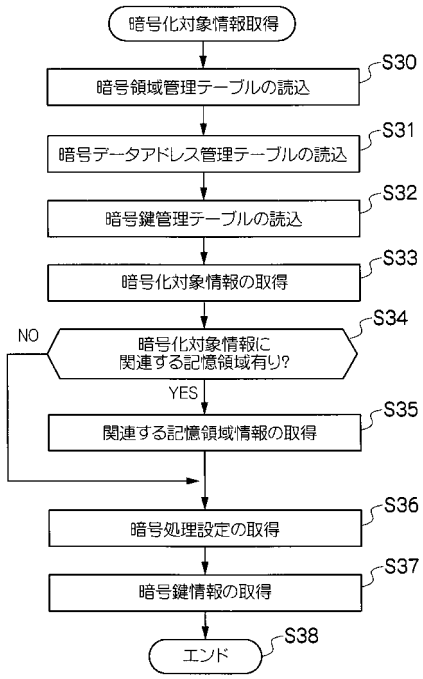
【図１４】

図14

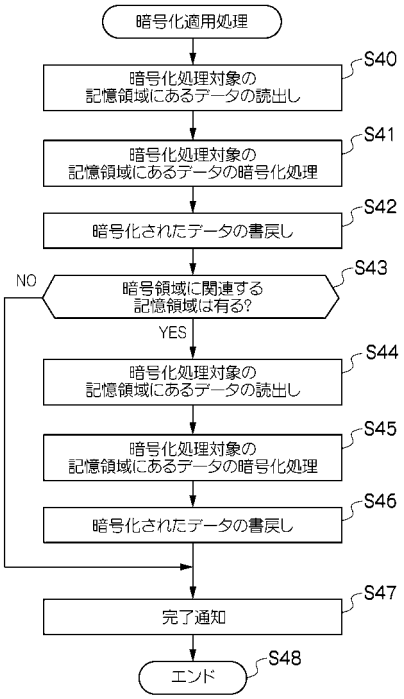


【図１５】

図15



【図１６】
図16


暗号化適用処理
S40
暗号化処理対象の
記憶領域にあるデータの読出し
S41
暗号化処理対象の
記憶領域にあるデータの暗号化処理
S42
暗号化されたデータの書戻し
S43
暗号領域に関連する
記憶領域は有る?
NO
YES
S44
暗号化処理対象の
記憶領域にあるデータの読出し
S45
暗号化処理対象の
記憶領域にあるデータの暗号化処理
S46
暗号化されたデータの書戻し
S47
完了通知
S48
エンド