(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4990089号
(P4990089)
(45)発行日　平成24年8月1日(2012.8.1)　(24)登録日　平成24年5月11日(2012.5.11)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 21/24 166E
G06F 3/06 (2006.01)　G06F 3/06 304F

請求項の数 15　(全 49 頁)

(21)出願番号　特願2007-266665(P2007-266665)
(22)出願日　平成19年10月12日(2007.10.12)
(65)公開番号　特開2009-98719(P2009-98719A)
(43)公開日　平成21年5月7日(2009.5.7)
審査請求日　平成22年1月4日(2010.1.4)

(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　100114236
弁理士　藤井　正弘
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100120260
弁理士　飯田　雅昭
(72)発明者　鬼頭　大介
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】格納データ暗号化機能内蔵ストレージ装置の暗号鍵をバックアップ及びリストアする計算機システム

(57)【特許請求の範囲】
【請求項１】
複数の計算機と、複数のストレージシステムと、前記複数の計算機の少なくとも一つ及び前記複数のストレージシステムに接続されるネットワークと、を備える計算機システムであって、
前記複数の計算機は、第１計算機及び第２計算機を含み、
前記各計算機は、ネットワークに接続される第１インタフェースと、前記第１インタフェースに接続される第１プロセッサと、前記第１プロセッサに接続される第１メモリと、を備え、
前記複数のストレージシステムは、第１ストレージシステム及び前記ネットワークを介して前記第１ストレージシステムに接続される第２ストレージシステムを含み、
前記各ストレージシステムは、前記ネットワークに接続される第２インタフェースと、前記第２インタフェースに接続される第２プロセッサと、前記第２プロセッサに接続される第２メモリと、を備え、
前記第１ストレージシステムは、前記第２計算機によって書き込まれたデータを格納する第１記憶領域を備え、
前記第２ストレージシステムは、前記第１ストレージシステムの第３記憶領域として前記第２計算機に提供され、前記第２計算機によって書き込まれたデータを格納する第２記憶領域を備え、
前記第１ストレージシステムは、

前記第２記憶領域と前記第３記憶領域とを対応付けるマッピング情報を保持し、
前記第２計算機から前記第１記憶領域への第１データの書き込み要求を受信すると、前記第１ストレージシステムが保持する第１暗号鍵を用いて前記第１データを暗号化し、前記暗号化された第１データを前記第１記憶領域に書き込み、
前記第２計算機から前記第３記憶領域への第２データの書き込み要求を受信すると、前記第１ストレージシステムが保持する第２暗号鍵を用いて前記第２データを暗号化し、前記暗号化された第２データの前記第２記憶領域への書き込み要求を前記第２ストレージシステムに送信し、
前記計算機システムは、暗号鍵と、前記暗号鍵に対応付けられた前記ストレージシステムの識別子と、を含むバックアップ情報を保持し、
前記バックアップ情報は、少なくとも、前記第１暗号鍵と、前記第１暗号鍵に対応付けられた前記第１ストレージシステムの識別子と、前記第２暗号鍵と、前記第２暗号鍵に対応付けられた前記第２ストレージシステムの識別子とを含み、
前記第１計算機は、前記バックアップ情報に含まれる少なくとも一つの前記暗号鍵と、前記少なくとも一つの暗号鍵に対応付けられた少なくとも一つの前記ストレージシステムの識別子と、を送信し、
前記第１ストレージシステムは、
前記第１計算機から受信した前記ストレージシステムの識別子が前記第１ストレージシステムの識別子である場合、前記第１計算機から受信した前記第１ストレージシステムの識別子に対応する前記暗号鍵を前記第１暗号鍵として保持し、
前記第１計算機から受信した前記ストレージシステムの識別子が前記第２ストレージシステムの識別子である場合、前記第１計算機から受信した前記第２ストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持し、
前記第１計算機から受信した前記ストレージシステムの識別子が前記第１ストレージシステムの識別子でない場合、前記第１計算機から受信した前記ストレージシステムの識別子に対応する前記暗号鍵を前記第１暗号鍵として前記第１ストレージシステムが保持することを禁止することを特徴とする計算機システム。
【請求項２】
前記第１ストレージシステムは、
前記前記第１暗号鍵の上書きが禁止される第１モード、又は、前記前記第１暗号鍵の上書きが許可される第２モードのいずれかに設定され、
前記第１計算機から受信した前記ストレージシステムの識別子が前記第１ストレージシステムの識別子である場合、前記第１ストレージシステムが前記第２モードに設定されているか否かを判定し、
前記第１ストレージシステムが前記第２モードに設定されている場合に限り、前記第１計算機から受信した前記暗号鍵を前記第１暗号鍵として保持することを特徴とする請求項１に記載の計算機システム。
【請求項３】
前記第２ストレージシステムは、
前記第１計算機から受信した前記ストレージシステムの識別子が前記第２ストレージシステムの識別子である場合、前記第１計算機から受信した前記第２ストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持し、
前記第２計算機から前記第２記憶領域への前記第２データの読み出し要求を受信すると、前記第２記憶領域から前記暗号化された第２データを読み出し、前記第２暗号鍵を用いて前記読み出された第２データを復号することを特徴とする請求項１に記載の計算機システム。
【請求項４】
前記第２ストレージシステムは、さらに、前記第１計算機から受信した前記第２ストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持した後に、前記第１計算機からの指示を受けて、前記第２計算機による前記第２記憶領域へのアクセスを

許可することを特徴とする請求項３に記載の計算機システム。
【請求項５】
前記第１計算機は、
前記第２記憶領域に格納されたデータが暗号化されているか否かを判定し、
前記第２記憶領域に格納されたデータが暗号化されている場合のみ、前記バックアップ情報に含まれる前記第２暗号鍵と、前記第２暗号鍵に対応付けられた前記第２ストレージシステムの識別子と、を送信することを特徴とする請求項３に記載の計算機システム。
【請求項６】
前記複数のストレージシステムは、さらに第３ストレージシステムを含み、
前記第３ストレージシステムは、
前記第１計算機から受信した前記ストレージシステムの識別子が前記第２ストレージシステムの識別子である場合、前記第１計算機から受信した前記第２ストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持し、
前記第２計算機から第３記憶領域への前記第２データの読み出し要求を受信すると、前記第２データの読み出し要求を前記第２ストレージシステムに送信し、
前記第２ストレージシステムから前記暗号化された第２データを受信すると、前記第２暗号鍵を用いて前記暗号化された第２データを復号することを特徴とする請求項１に記載の計算機システム。
【請求項７】
前記第３ストレージシステムは、さらに、前記第１計算機から受信した前記第２ストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持した後に、前記第１計算機からの指示を受けて、前記第２計算機による前記第３記憶領域へのアクセスを許可することを特徴とする請求項６に記載の計算機システム。
【請求項８】
前記第１計算機は、
前記第２記憶領域に格納されたデータが暗号化されているか否かを判定し、
前記第２記憶領域に格納されたデータが暗号化されている場合のみ、前記バックアップ情報に含まれる前記第２暗号鍵と、前記第２暗号鍵に対応付けられた前記第２ストレージシステムの識別子と、を送信することを特徴とする請求項６に記載の計算機システム。
【請求項９】
前記第１計算機は、アクセス権設定指示を前記第２ストレージシステムに送信し、
前記第２ストレージシステムは、前記アクセス権設定指示に基づいて、前記第３ストレージシステムが前記第２記憶領域にアクセスすることを許可することを特徴とする請求項６に記載の計算機システム。
【請求項１０】
前記第１計算機が前記バックアップ情報を保持することを特徴とする請求項１に記載の計算機システム。
【請求項１１】
前記複数の計算機は、さらに、第３計算機を含み、
前記第３計算機が前記バックアップ情報を保持し、
前記第１計算機が前記バックアップ情報に含まれる少なくとも一つの前記暗号鍵と、前記少なくとも一つの暗号鍵に対応付けられた少なくとも一つの前記ストレージシステムの識別子と、を送信する手順は、前記第１計算機が前記第３計算機に前記バックアップ情報の送信指示を送信し、前記第３計算機が前記バックアップ情報に含まれる少なくとも一つの前記暗号鍵と、前記少なくとも一つの暗号鍵に対応付けられた少なくとも一つの前記ストレージシステムの識別子と、を送信することによって実行されることを特徴とする請求項１に記載の計算機システム。
【請求項１２】
複数の計算機と接続されるストレージシステムであって、
前記複数の計算機は、第１計算機及び第２計算機を含み、

前記ストレージシステムは、
前記複数の計算機又は他のストレージシステムの少なくとも一つに接続される第１インタフェースと、前記第１インタフェースに接続される第１プロセッサと、前記第１プロセッサに接続される第１メモリと、を備え、
前記第２計算機によって書き込まれたデータを格納する第１記憶領域を備え、
前記第２計算機から前記第１記憶領域への第１データの書き込み要求を受信すると、前記ストレージシステムが保持する第１暗号鍵を用いて前記第１データを暗号化し、前記暗号化された第１データを前記第１記憶領域に書き込み、
前記第２計算機から第２記憶領域への第２データの書き込み要求を受信すると、前記ストレージシステムが保持する第２暗号鍵を用いて前記第２データを暗号化し、前記暗号化された第２データの書き込み要求を、前記ストレージシステムに接続された前記他のストレージシステムに送信し、
前記第１暗号鍵と、前記第１暗号鍵に対応付けられた前記ストレージシステムの識別子と、前記第２暗号鍵と、前記第２暗号鍵に対応付けられた前記他のストレージシステムの識別子とをバックアップ情報として前記第１計算機に送信し、
少なくとも一つの暗号鍵と、前記少なくとも一つの暗号鍵に対応付けられた少なくとも一つのストレージシステムの識別子と、を含むバックアップ情報を受信し、
前記受信したストレージシステムの識別子が自ストレージシステムの識別子である場合、前記自ストレージシステムの識別子に対応する前記暗号鍵を前記第１暗号鍵として保持し、
前記受信したストレージシステムの識別子が自ストレージシステムに接続された前記他のストレージシステムの識別子である場合、前記他のストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持し、
前記受信したストレージシステムの識別子が自ストレージシステムの識別子でない場合、前記受信したストレージシステムの識別子に対応する前記暗号鍵を前記第１暗号鍵として前記自ストレージシステムが保持することを禁止することを特徴とするストレージシステム。
【請求項１３】
前記ストレージシステムは、前記他のストレージシステムが前記第１計算機から受信したアクセス権設定指示に基づいて、前記ストレージシステムの前記第２記憶領域へのアクセスを許可すると、前記第２記憶領域へのアクセスが可能になることを特徴とする請求項１２に記載のストレージシステム。
【請求項１４】
前記ストレージシステムは、
前記受信したストレージシステムの識別子が、自ストレージシステムの識別子又は自ストレージシステムに接続された前記他のストレージシステムの識別子のいずれでもない場合、前記受信したストレージシステムの識別子を有する前記他のストレージシステムの前記第２記憶領域へのアクセスが可能か否かを判定し、
アクセス可能な場合、前記受信したストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持することを特徴とする請求項１２に記載のストレージシステム。
【請求項１５】
前記ストレージシステムは、
前記前記第１暗号鍵の上書きが禁止される第１モード、又は、前記前記第１暗号鍵の上書きが許可される第２モードのいずれかに設定され、
前記第１計算機から受信したストレージシステムの識別子が自ストレージシステムの識別子である場合、前記自ストレージシステムが前記第２モードに設定されているか否かを判定し、
前記自ストレージシステムが前記第２モードに設定されている場合に限り、前記第１計算機から受信した前記暗号鍵を前記第１暗号鍵として保持することを特徴とする請求項１

２に記載のストレージシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本願明細書で開示される技術は、計算機が使用するデータを格納するストレージ装置を含む計算機システムに関する。本願明細書で開示される技術は、特に、ストレージ装置が記憶媒体に格納されるデータを暗号化する機能、及び、記憶媒体から読み出されたデータを復号する機能を備える場合に、その暗号化及び復号に使用される暗号鍵をバックアップ及びリストアする技術に関する。

【背景技術】

【０００２】

近年、ストレージ装置、計算機及び管理計算機をＦｉｂｒｅ　Ｃｈａｎｎｅｌのような専用線で接続するストレージエリアネットワーク（ＳＡＮ）の普及に伴い、計算機システムの大規模化が進んでいる。上記計算機システムの膨大化するデータを効率的に管理する技術が開発されている。

【０００３】

例えば特許文献１では、ストレージ仮想化技術が開示されている。この技術によれば、第１のストレージ装置が一台以上の第２のストレージ装置に接続され、第２のストレージ装置の記憶領域が第１のストレージ装置の記憶領域として計算機へ提供される。

【０００４】

特許文献１の技術によれば、第２のストレージ装置の記憶領域を第１のストレージ装置が集約管理することで、計算機システムの管理コストを低減することができる。

【０００５】

また近年、ディスク盗難等に起因した情報漏洩事件の増加に伴い、データのセキュアな保存及び管理への関心が高まっている。例えば特許文献２によれば、ストレージ装置は、記憶領域の暗号化機能を備え、記憶領域に読み書きするデータを暗号化することができる。

【０００６】

特許文献２の技術によれば、ディスク盗難等の被害を受けた場合であっても、データ漏洩を防止することができる。

【０００７】

上記のような暗号化機能を備えるストレージ装置においては、その暗号鍵の管理が重要である。例えば、ストレージ装置の故障やユーザの誤操作などで暗号鍵を消失した場合、ストレージ装置は暗号化された記憶領域のデータを復号できなくなる。このような事態に対処するため、暗号鍵をストレージ装置外又は装置内へバックアップしておき、暗号鍵が消失した場合はバックアップした暗号鍵をストレージ装置へリストアすることが考えられる。

【０００８】

但し、暗号鍵のリストアにあたっては次のことに留意する必要がある。バックアップした暗号鍵のうち、誤った暗号鍵をストレージ装置へリストアしてデータを読み書きすると、データが壊れてしまう。このため、暗号鍵の誤リストアを防止すること、即ち、本当に正しい暗号鍵をストレージ装置にリストアしているか否かを検証することが必要である。

【０００９】

上記の検証に関連する従来技術として、特許文献３のような技術が開示されている。特許文献３によれば、ＵＳＢメモリ等の外部記憶媒体において、記憶媒体の接続先が正当な計算機であればデータの利用が許可され、不当な計算機であればデータの利用が禁止される。

【００１０】

特許文献３の技術のような、データの利用先に基づいてデータの利用可否を判断する方法によれば、例えば暗号機能を持つストレージ装置で暗号鍵をリストアする際に、その暗

号鍵が自装置のものであればリストアを許可し、自装置以外のストレージ装置の暗号鍵であればリストアを拒否するといった判断をすることができる。
【特許文献１】特開２００５－１１２７７号公報
【特許文献２】特開２００７－２８５０２号公報
【特許文献３】特開２００７－１４８７６２号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
上記の特許文献３によれば、管理者がデータの利用先を誤って登録した場合は暗号鍵の誤リストアを防止することができない。このため暗号鍵をリストアされるストレージ装置側に暗号鍵の誤リストア防止の仕組みを持たせる必要がある。
【００１２】
さらに、仮想化機能を備えるストレージ装置では、以下の課題が生じる。ここで、第１のストレージ装置が第２のストレージ装置の記憶領域を仮想化する、階層構成の計算機システムを例として仮定する。第１のストレージ装置がストレージ装置ごとの又は記憶領域ごとの暗号鍵を持ち、第１のストレージ装置が自装置用の暗号鍵を使って自装置の記憶領域を暗号化する。さらに、第１のストレージ装置が第２のストレージ装置用の暗号鍵を使って第２のストレージ装置の記憶領域を暗号化する。なお、記憶領域を暗号化するとは、その記憶領域に格納されている（及びこれから格納される）データを暗号化することを意味する。
【００１３】
この例において、第１のストレージ装置が故障したとき、第２のストレージ装置を第３のストレージ装置につなぎかえて、第３のストレージ装置が第２のストレージ装置の暗号化された記憶領域のデータを復号することが考えられる。この場合、第３のストレージ装置に、第１のストレージ装置で使っていた暗号鍵をリストアする必要がある。しかし、第３のストレージ装置に既に自装置用の暗号鍵（すなわち、第３のストレージ装置内の記憶領域に使用される暗号鍵）が設定されている場合、第１のストレージ装置からバックアップされた暗号鍵を第３のストレージ装置にリストアすると、第３のストレージ装置の自装置用の暗号鍵が、第１のストレージ装置の自装置用の暗号鍵（すなわち、第１のストレージ装置内の記憶領域に使用される暗号鍵）で上書きされる。その結果、第３のストレージ装置内の記憶領域から読み出されたデータが、第１のストレージ装置で使用されていた暗号鍵で復号されるため、データが壊れてしまう。
【００１４】
このようなデータ破壊を防ぐため、自ストレージ装置からバックアップされた暗号鍵以外のリストアを禁止することが考えられる。しかしその場合、上記のような階層構成の計算機システムでは、第１のストレージ装置が故障した場合、仮想化された第２のストレージ装置内の暗号化された記憶領域のデータを復号することができない。
【００１５】
本発明は、上記の点を鑑みてなされたものであり、本発明の目的は、上記のような階層構成を有する計算機システムにおいて、第１のストレージ装置が故障した場合、バックアップされている暗号鍵を正しくリストアすることによって、データを破壊することなく、第２のストレージ装置の暗号化された記憶領域のデータを復号可能にすることである。
【課題を解決するための手段】
【００１６】
本願で開示する代表的な発明は、複数の計算機と、複数のストレージシステムと、前記複数の計算機の少なくとも一つ及び前記複数のストレージシステムに接続されるネットワークと、を備える計算機システムであって、前記複数の計算機は、第１計算機及び第２計算機を含み、前記各計算機は、ネットワークに接続される第１インタフェースと、前記第１インタフェースに接続される第１プロセッサと、前記第１プロセッサに接続される第１メモリと、を備え、前記複数のストレージシステムは、第１ストレージシステム及び前記

ネットワークを介して前記第１ストレージシステムに接続される第２ストレージシステムを含み、前記各ストレージシステムは、前記ネットワークに接続される第２インタフェースと、前記第２インタフェースに接続される第２プロセッサと、前記第２プロセッサに接続される第２メモリと、を備え、前記第１ストレージシステムは、前記第２計算機によって書き込まれたデータを格納する第１記憶領域を備え、前記第２ストレージシステムは、前記第１ストレージシステムの第３記憶領域として前記第２計算機に提供され、前記第２計算機によって書き込まれたデータを格納する第２記憶領域を備え、前記第１ストレージシステムは、前記第２記憶領域と前記第３記憶領域とを対応付けるマッピング情報を保持し、前記第２計算機から前記第１記憶領域への第１データの書き込み要求を受信すると、前記第１ストレージシステムが保持する第１暗号鍵を用いて前記第１データを暗号化し、前記暗号化された第１データを前記第１記憶領域に書き込み、前記第２計算機から前記第３記憶領域への第２データの書き込み要求を受信すると、前記第１ストレージシステムが保持する第２暗号鍵を用いて前記第２データを暗号化し、前記暗号化された第２データの前記第２記憶領域への書き込み要求を前記第２ストレージシステムに送信し、前記計算機システムは、暗号鍵と、前記暗号鍵に対応付けられた前記ストレージシステムの識別子と、を含むバックアップ情報を保持し、前記バックアップ情報は、少なくとも、前記第１暗号鍵と、前記第１暗号鍵に対応付けられた前記第１ストレージシステムの識別子と、前記第２暗号鍵と、前記第２暗号鍵に対応付けられた前記第２ストレージシステムの識別子とを含み、前記第１計算機は、前記バックアップ情報に含まれる少なくとも一つの前記暗号鍵と、前記少なくとも一つの暗号鍵に対応付けられた少なくとも一つの前記ストレージシステムの識別子と、を送信し、前記第１ストレージシステムは、前記第１計算機から受信した前記ストレージシステムの識別子が前記第１ストレージシステムの識別子である場合、前記第１計算機から受信した前記第１ストレージシステムの識別子に対応する前記暗号鍵を前記第１暗号鍵として保持し、前記第１計算機から受信した前記ストレージシステムの識別子が前記第２ストレージシステムの識別子である場合、前記第１計算機から受信した前記第２ストレージシステムの識別子に対応する前記暗号鍵を前記第２暗号鍵として保持し、前記第１計算機から受信した前記ストレージシステムの識別子が前記第１ストレージシステムの識別子でない場合、前記第１計算機から受信した前記ストレージシステムの識別子に対応する前記暗号鍵を前記第１暗号鍵として前記第１ストレージシステムが保持することを禁止することを特徴とする。

【発明の効果】

【００１７】

本発明の一実施形態によれば、仮想化機能を備えるストレージ装置が故障しても、他の仮想化機能を備えるストレージ装置に暗号鍵を誤ることなくリストアすることができる。その結果、データ破壊を起こすことなく、暗号化された記憶領域のデータを復号することができる。

【発明を実施するための最良の形態】

【００１８】

以下、本発明の第１、第２及び第３の実施形態を説明する。なお、以下に説明する実施形態は一例であって、本発明はこれに限定されるものではない。

【００１９】

図１から図１７を用いて第１の実施形態を説明する。

【００２０】

＜システム構成＞

図１は、本発明の第１の実施形態の計算機システムのハードウェア構成を示すブロック図である。

【００２１】

計算機システムは、１台以上の計算機１００、ファイバチャネルスイッチ（以下ＦＣスイッチと記載する）１１０、ストレージ装置１２０Ａ及び１２０Ｂ（以下、これらを総称してストレージ装置１２０とも記載する）、１台以上の仮想先ストレージ装置１３０及び

管理計算機１４０を備える。

【００２２】

計算機１００、ストレージ装置１２０及び仮想先ストレージ装置１３０は、それぞれＦＣインタフェース（以下ＦＣＩ／Ｆ）１０３、１２１及び１３１を介してＦＣスイッチ１１０に接続される。ＦＣスイッチ１１０、ストレージ装置１２０及び仮想先ストレージ装置１３０は、それぞれ管理Ｉ／Ｆ１１１、１２６及び１３６を介してＩＰネットワーク経由で管理計算機１４０に接続され、管理計算機１４０によって管理される。

【００２３】

計算機１００は、ＣＰＵ１０１及びＣＰＵ１０１に接続されたメモリ１０２を備える。メモリ１０２には、ＣＰＵ１０１が実行するプログラム及びストレージ装置１２０に読み書きされるデータが保持される。さらに、計算機１００は、ＦＣスイッチ１１０と接続される１以上のＦＣＩ／Ｆ１０３、及び、管理計算機１４０とＩＰネットワーク経由で接続される１以上の管理Ｉ／Ｆ１０４を備える。ＦＣＩ／Ｆ１０３及び管理Ｉ／Ｆ１０４は、ＣＰＵ１０１と接続される。

【００２４】

ストレージ装置１２０は、ＦＣスイッチ１１０と接続される１以上のＦＣＩ／Ｆ１２１と、１以上のＣＰＵ１２２と、１以上のキャッシュメモリ１２３と、１以上の制御メモリ１２４と、１以上の記憶領域１２５と、１以上の管理Ｉ／Ｆ１２６と、を備える。これらの各部は、例えば内部バス等によって相互に接続されている。

【００２５】

ＦＣＩ／Ｆ１２１は、ＦＣスイッチ１１０と接続される１以上のポート（図示省略）を備える。

【００２６】

ストレージ装置１２０のＣＰＵ１２２は、ＦＣＩ／Ｆ１２１を介して計算機１００からのデータの読み書きの要求を受け取り、要求されたデータを記憶領域１２５に読み書きする。記憶領域１２５とは、ＣＰＵ１２２によってストレージ装置１２０のディスク装置などの物理的デバイスに対応付けて管理される論理的なデバイスである。計算機１００はこの記憶領域１２５を認識して、ストレージ装置１２０に対してデータの読み書きを要求する。

【００２７】

ストレージ装置１２０は、仮想先ストレージ装置１３０の記憶領域１３５を自ストレージ装置１２０の記憶領域１２５として仮想化することができる。

【００２８】

ストレージ装置１２０が記憶領域１３５を記憶領域１２５として仮想化していない場合、記憶領域１２５は、ストレージ装置１２０内の物理的な記憶領域（例えば図示しないハードディスクドライブの記憶領域）に対応付けられる。この場合、計算機１００から記憶領域１２５へのデータの読み書き要求を受けると、ストレージ装置１２０は、記憶領域１２５に対応付けられたストレージ装置１２０内の物理的な記憶領域へのデータの書き込み又は読み出しを実行し、その結果を計算機１００に応答する。

【００２９】

一方、ストレージ装置１２０が記憶領域１３５を記憶領域１２５として仮想化している場合、記憶領域１２５は、ストレージ装置１２０内の物理的な記憶領域と対応付けられる代わりに、仮想先ストレージ装置１３０の記憶領域１３５と対応付けられる。この場合、計算機１００から記憶領域１２５へのデータの読み書き要求を受けると、ストレージ装置１２０は、受けた要求を、記憶領域１３５へのデータの読み書き要求に変換して、仮想先ストレージ装置１３０に送信する。

【００３０】

仮想先ストレージ装置１３０は、ストレージ装置１２０から受信した要求に従って、記憶領域１３５に対応付けられた仮想先ストレージ装置１３０内の物理的な記憶領域へのデータの読み書きを実行し、その結果をストレージ装置１２０に応答する。ストレージ装置

１２０は、仮想先ストレージ装置１３０から応答を受信すると、その応答をストレージ装置１２０からの応答に変換して、計算機１００に送信する。

【００３１】

このように、記憶領域１３５がストレージ装置１２０によって仮想化されている場合、記憶領域１３５は、仮想先記憶領域（又は仮想先ＬＵ）とも記載される。一方、記憶領域１３５を仮想化する記憶領域１２５は、仮想記憶領域（又は仮想ＬＵ）とも記載される。一方、記憶領域１２５が、ストレージ装置１２０内の物理的な記憶領域と対応付けられている場合、記憶領域１２５は、実記憶領域（又は実ＬＵ）とも記載される。

【００３２】

図１の例では、一つの記憶領域１２５及び一つの記憶領域１３５のみが記載されている。しかし、ストレージ装置１２０及び仮想先ストレージ装置１３０は、それぞれ、複数の記憶領域１２５及び複数の記憶領域１３５を含んでもよい。この場合、例えば、複数の記憶領域１２５のうち少なくとも一つが実記憶領域１２５であり、残りの記憶領域１２５が、記憶領域１３５を仮想化する仮想記憶領域１２５であってもよい。

【００３３】

また、ストレージ装置１２０のＣＰＵ１２２は、管理Ｉ／Ｆ１２６を介して管理計算機１４０からストレージ装置１２０の運用管理操作の要求を受け取り、要求された管理操作を実行する。ＣＰＵ１２２は、管理操作の結果及びストレージ装置１２０の構成情報等を管理計算機１４０に送信する。

【００３４】

キャッシュメモリ１２３には、計算機１００から受信したデータ及び記憶領域１２５から頻繁に読み出されるデータが格納される。

【００３５】

制御メモリ１２４には、記憶領域１２５の構成情報、記憶領域１２５の属性（例えば記憶領域１２５が暗号化されているか平文であるか）、及び、暗号鍵等の情報が格納される。以下、記憶領域１２５等が暗号化されていることを「暗号ｏｎ」、記憶領域１２５等が暗号化されていない（すなわち平文データを格納している）ことを「暗号ｏｆｆ」とも記載する。

【００３６】

ストレージ装置１２０は、データの暗号化・復号化機能を備える。すなわち、ストレージ装置１２０は、暗号化された記憶領域へのデータ書き込み要求を受けると、要求されたデータを暗号化して記憶領域に書き込む。そして、暗号化された記憶領域からのデータ読み出し要求を計算機１００から受けると、ストレージ装置１２０は、要求されたデータを記憶領域から読み出し、読み出されたデータを復号化して計算機１００に応答する。

【００３７】

仮想先ストレージ装置１３０は、ＦＣスイッチ１１０と接続される１以上のＦＣＩ／Ｆ１３１と、１以上のＣＰＵ１３２と、１以上のキャッシュメモリ１３３と、１以上の制御メモリ１３４と、１以上の記憶領域１３５と、１以上の管理Ｉ／Ｆ１３６と、を備える。これらの各部は、例えば内部バス等によって相互に接続されている。

【００３８】

ストレージ装置１３０のＣＰＵ１３２は、ＦＣＩ／Ｆ１３１を介して計算機１００又はストレージ装置１２０からのデータの読み書きの要求を受け取り、要求されたデータを記憶領域１３５に読み書きする。またＣＰＵ１３２は、管理Ｉ／Ｆ１３６を介して管理計算機１４０から仮想先ストレージ装置１３０の運用管理操作の要求を受け取り、要求された管理操作を実行する。

【００３９】

仮想先ストレージ装置１３０は図１に示すものに限定されず、例えばデータの暗号化・復号化機能を備えているストレージ装置又は備えていないストレージ装置等、機能、性能又は構成の異なるストレージ装置であってもよい。

【００４０】

管理計算機１４０は、ＣＰＵ１４１、メモリ１４２及び管理Ｉ／Ｆ１４３を備える。管理Ｉ／Ｆ１４３は、ＩＰネットワーク経由で計算機１００及びＦＣスイッチ１１０と接続される。

【００４１】

管理計算機１４０は、管理計算機１４０の図示しない磁気ディスク装置等の不揮発記録媒体に記録された、ストレージ装置や計算機の管理のためのプログラムを、管理計算機１４０の起動時等にメモリ１４２にロードする。ＣＰＵ１４１はそれらのロードしたプログラムを実行することで、ストレージ装置１２０及び仮想先ストレージ装置１３０の構成情報の取得、障害検知及び性能監視等を行うことができる。管理者は管理計算機１４０を使うことで、計算機システム全体の運用管理を行うことができる。

【００４２】

尚、上記のプログラムは、磁気ディスク装置以外の記憶媒体（例えばＣＤ－ＲＯＭ又はフロッピーディスク等）に記録されてもよい。上記のプログラムは、当該記憶媒体から管理計算機１４０にロードして実行されてもよいし、ネットワークを通じて他の記憶媒体からロードされてもよい。

【００４３】

＜ソフトウェア構成＞

次に、本実施形態のストレージ装置１２０、仮想先ストレージ装置１３０及び管理計算機１４０のソフトウェア構成について説明する。

【００４４】

図２は、本発明の第１の実施形態の計算機システムのソフトウェア構成の一例を示す説明図である。

【００４５】

ストレージ装置１２０の制御メモリ１２４には、記憶領域１２５の識別子及び容量等、ストレージ装置１２０の構成管理のための構成情報と、暗号鍵の管理情報と、データ読み書きのプログラム及び暗号設定のプログラム等のプログラム情報と、が格納される。最初に構成情報について説明し、その後、暗号鍵の管理情報及びプログラム情報について説明する。

【００４６】

制御メモリ１２４には構成情報として、記憶領域（以下、ＬＵ：Ｌｏｇｉｃａｌ Ｕｎｉｔとも記載される）管理情報２０１、仮想ＬＵマッピング情報２０２、ストレージ装置機種・製造番号管理情報２０３及び暗号鍵管理情報２０４が格納される。

【００４７】

最初に、ＬＵ管理情報２０１について説明する。

【００４８】

図３は、本発明の第１の実施形態のＬＵ管理情報２０１の一例を示す説明図である。

【００４９】

ＬＵ管理情報２０１は項目３０１～項目３０７の７つのデータ項目から構成される。

【００５０】

項目３０１には、ストレージ装置１２０のポート番号が格納される。ポート番号はストレージ装置１２０のＦＣＩ／Ｆ１２１が備える各ポート（図示省略）に割当てられた、一意に識別可能な値である。ストレージ装置１２０はポートごとにＬＵを定義することができる。計算機１００はこのポートを介してＬＵへアクセスする。ストレージ装置１２０は複数のポートを持つことができる。

【００５１】

項目３０２には、記憶領域（ＬＵ）１２５及び１３５を識別するためのＬＵ番号が格納される。ＬＵ番号はポートごとに定義することができる。計算機１００は、ポート番号及びＬＵ番号を使ってアクセス先を指定する。

【００５２】

項目３０３には、ＬＵの容量が格納される。

【００５３】
項目３０４には、ＬＵへのアクセスが許可されている計算機１００の識別情報が格納される。項目３０４には、例えば、ＬＵへのアクセスが許可されている計算機１００のポートに割当てられているＷＷＮ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎａｍｅ）等の値が格納される。
【００５４】
項目３０５には、各ＬＵがストレージ装置１２０内の物理デバイスを使用しているＬＵ（すなわち実ＬＵ）であるか、仮想先ストレージ装置１３０内のＬＵを仮想化することによって作成されたＬＵ（すなわち仮想ＬＵ）であるかを示す情報が格納される。
【００５５】
項目３０６には、ＬＵの暗号Ｏｎ／Ｏｆｆを示す情報が格納される。あるＬＵが暗号化されている場合、そのＬＵに対応する項目３０６に「Ｏｎ」が格納され、暗号化されていない場合は「Ｏｆｆ」が格納される。
【００５６】
項目３０７には、各ＬＵに対応する鍵ＩＤが格納される。鍵ＩＤは、あるＬＵが暗号化される場合にその暗号化に使用される暗号鍵を識別するためのＩＤであり、各暗号鍵をストレージ装置１２０内で一意に識別する値である。ＬＵが暗号化されない場合、この項目３０７の値は定義されない。
【００５７】
この鍵ＩＤは後述の鍵ＩＤ６０１と同義であり、このＩＤから暗号鍵の詳細情報を取得することができる。
【００５８】
次に、仮想ＬＵマッピング情報２０２について説明する。
【００５９】
図４は、本発明の第１の実施形態の仮想ＬＵマッピング情報２０２の一例を示す説明図である。
【００６０】
仮想ＬＵマッピング情報２０２は項目４０１～項目４０５の５つのデータ項目から構成される。
【００６１】
項目４０１には、ストレージ装置１２０のポート番号が格納される。
【００６２】
項目４０２には、ストレージ装置１２０の各ポートにおいて定義されている仮想ＬＵのＬＵ番号が格納される。
【００６３】
項目４０３には、仮想先ストレージ装置１３０を一意に識別する仮想先ストレージ装置機種・製造番号が格納される。
【００６４】
項目４０４には、ストレージ装置１２０の仮想ＬＵに対応付けられた仮想先ストレージ装置１３０のポート番号が格納される。ストレージ装置１２０はこのポート番号及びストレージ装置１２０が仮想化するＬＵ番号を指定して仮想先ストレージ装置１３０内のＬＵにアクセスする。
【００６５】
項目４０５には、ストレージ装置１２０によって仮想化された仮想先ストレージ装置１３０内のＬＵを識別するための、仮想先装置内ＬＵ番号が格納される。当該ＬＵ番号は、仮想先ストレージ装置１３０内で定義されているＬＵ番号である。
【００６６】
次に、ストレージ装置機種・製造番号管理情報２０３について説明する。
【００６７】
図５は、本発明の第１の実施形態のストレージ装置機種・製造番号管理情報２０３の一例を示す説明図である。

【００６８】
ストレージ装置機種・製造番号管理情報２０３は項目５０１～項目５０４の４つのデータ項目から構成される。
【００６９】
項目５０１には、ストレージ装置１２０の装置機種及び製造番号が格納される。
【００７０】
項目５０２には、ストレージ装置１２０の管理Ｉ／Ｆ１２６に設定された、ストレージ装置１２０の識別のためのＩＰアドレス又はホスト名が格納される。
【００７１】
項目５０３には、ストレージ装置１２０の動作モードを示す情報が格納される。通常時は項目５０３に通常モードが設定されるが、後述のシステムオプションモードが設定される場合、項目５０３に「システムオプションモード」が格納される。
【００７２】
項目５０４には、ストレージ装置１２０によって仮想化されたＬＵを含む仮想先ストレージ装置１３０の装置機種・製造番号が格納される。１以上のストレージ装置１２０及び仮想先ストレージ装置１３０からなる計算機システムでは、この装置機種・製造番号によって、各ストレージ装置１２０及び仮想先ストレージ装置１３０を一意に識別することができる。
【００７３】
ストレージ装置１２０は、以上３つの情報を構成情報として管理し、ストレージ装置１２０の構成管理に使用する。さらに、構成情報は、上記以外の情報、例えばＬＵの状態（コピー状態等）を示す情報を含んでもよい。
【００７４】
次に、ストレージ装置１２０の暗号鍵管理情報２０４について説明する。
【００７５】
図６は、本発明の第１の実施形態の暗号鍵管理情報２０４の一例を示す説明図である。
【００７６】
暗号鍵管理情報２０４は項目６０１～項目６０７の７つのデータ項目から構成される。
【００７７】
項目６０１には、ストレージ装置１２０内で暗号鍵を識別するために使用される鍵ＩＤが格納される。
【００７８】
項目６０２には、暗号鍵のデータ（すなわち、暗号鍵として使用されるデータ列）が格納される。
【００７９】
項目６０３には、暗号鍵の長さを示す値が格納される。
【００８０】
項目６０４には、各暗号鍵がどの暗号アルゴリズムやモードを使うものであるかを示す、アルゴリズムの情報が格納される。例えば、ＡＥＳのＥＣＢモードでデータが暗号化される場合、項目６０４には「ＡＥＳ－ＥＣＢ」が格納される。
【００８１】
項目６０５には、暗号鍵の適用先装置を示す情報が格納される。例えば暗号鍵がストレージ装置１２０内の実ＬＵの暗号化に使用される場合、その暗号鍵に対応する項目６０５には、その暗号鍵が自装置用のものであることを示す値（図６の例では「自」）が格納される。一方、暗号鍵が仮想先ストレージ装置１３０内の仮想先ＬＵの暗号化に使用される場合、その暗号鍵に対応する項目６０５には、その暗号鍵が仮想先装置用のものであることを示す値（図６の例では「仮想先」）が格納される。
【００８２】
項目６０６には、仮想先ストレージ装置１３０の装置機種・製造番号が格納される。
【００８３】

項目６０７には、暗号鍵が適用される範囲を示す情報が格納される。例えば、一つの暗号鍵が、一つのストレージ装置１２０又は一つの仮想先ストレージ装置１３０内の、「暗号Ｏｎ」に設定された全てのＬＵ１３５の暗号化に使用される場合、その暗号鍵及びその装置に対応する項目６０７に「装置」が格納される。一方、一つの暗号鍵が一つのＬＵの暗号化に使用される場合、その暗号鍵に対応する項目６０７に、その暗号鍵が適用されるＬＵのＬＵ番号が格納される。

【００８４】

本実施形態は主に、ストレージ装置１２０内のＬＵ１２５に使用される暗号鍵と仮想先ストレージ装置１３０内のＬＵ１３５に使用される暗号鍵とが異なる場合について説明する。ストレージ装置ごとに暗号鍵を別にする理由は、仮に全てのストレージ装置の暗号鍵を同じにすると、一つのストレージ装置から暗号鍵が漏洩した場合、その他のストレージ装置の暗号鍵も全て知られてしまいセキュリティ的に好ましくないためである。但し、上記の形態に限定するわけではなく、全てのストレージ装置で同じ暗号鍵を使う場合にも本実施形態を適用することができる。

【００８５】

次に、ストレージ装置１２０のプログラム情報について説明する。図２に示すように、ストレージ装置１２０のプログラム情報は、Ｉ／Ｏ処理プログラム２０５、暗号設定プログラム２０６、暗号鍵・暗号設定情報バックアッププログラム２０７、暗号鍵・暗号設定情報リストアプログラム２０８及びストレージ管理プログラム２０９の５つのプログラムを含む。これらのプログラムは、ＣＰＵ１２２によって実行される。したがって、以下の説明においてこれらのプログラムが実行する処理は、実際にはＣＰＵ１２２によって実行される。

【００８６】

Ｉ／Ｏ処理プログラム２０５は計算機１００からの指示を受けて実行される。一方、その他の４つのプログラムは管理計算機１４０を使う管理者からの指示を受けて実行される。

【００８７】

Ｉ／Ｏ処理プログラム２０５は、計算機１００からのデータ読み書き要求を受け、ストレージ装置１２０又は仮想先ストレージ装置１３０の記憶領域にデータを読み書きする。

【００８８】

暗号設定プログラム２０６は、ストレージ装置１２０又は仮想先ストレージ装置１３０の記憶領域の暗号設定を行う。例えば記憶領域の暗号設定をＯｎにした場合、その記憶領域に暗号鍵が設定され、以降Ｉ／Ｏ処理プログラムはその暗号鍵を用いて計算機１００からのデータを暗号化して記憶領域に書き込み、読み出されたデータを復号化する。

【００８９】

暗号鍵・暗号設定情報バックアッププログラム２０７は、ストレージ装置１２０が保持する暗号鍵及び構成情報（具体的には、ＬＵ管理情報２０１、仮想ＬＵマッピング情報２０２及び暗号鍵管理情報２０４として保持されている情報）を、管理計算機１４０にバックアップする。以下の説明において、これらの情報を暗号鍵・暗号設定情報とも記載する。

【００９０】

暗号鍵・暗号設定情報リストアプログラム２０８は、管理計算機１４０から受信したバックアップファイルをストレージ装置１２０にリストア可能か否か判定し、リストアを許可又は禁止する。

【００９１】

ストレージ管理プログラム２０９は、ストレージ装置１２０が備えるその他の機能、例えば計算機１００との間のパスの設定及び記憶領域のコピー等、を実行する。以上がストレージ装置１２０のソフトウェア構成である。

【００９２】

次に、仮想先ストレージ装置１３０のソフトウェア構成について説明する。

【００９３】
仮想先ストレージ装置１３０の制御メモリ１３４には、ストレージ装置１２０のＬＵ管理情報２０１と同様、仮想先ストレージ装置内のＬＵ番号や容量、アクセス可能な計算機の情報等を管理するＬＵ管理情報２２１が格納される。
【００９４】
さらに、制御メモリ１３４には、プログラム情報として、Ｉ／Ｏ処理プログラム２２３及びストレージ管理プログラム２２４が格納される。これらのプログラムは、ＣＰＵ１３２によって実行される。したがって、以下の説明においてこれらのプログラムが実行する処理は、実際にはＣＰＵ１３２によって実行される。
【００９５】
Ｉ／Ｏ処理プログラム２２３は、計算機１００又はストレージ装置１２０からのデータ読み書き要求を処理する。ストレージ管理プログラム２２４は、管理計算機１４０から受けた指示に従って、仮想先ストレージ装置内の機能、例えば計算機とのパスの設定等、を実行する。なお、仮想先ストレージ装置１３０のソフトウェア構成がストレージ装置１２０のソフトウェア構成と同じであってもよい。
【００９６】
次に管理計算機１４０のソフトウェア構成について説明する。管理計算機１４０のメモリ１４２には、暗号鍵・暗号設定情報バックアップ情報２４１、ストレージ管理情報２４２及び管理者認証情報２４３が格納される。
【００９７】
暗号鍵・暗号設定情報バックアップ情報２４１は、ストレージ装置１２０からバックアップされた暗号鍵及び暗号設定に関する情報である。
【００９８】
ストレージ管理情報２４２は、ストレージ装置１２０及び仮想先ストレージ装置１３０を管理するための情報である。通常、管理計算機１４０は、ストレージ管理情報２４２を用いてストレージ装置１２０等を管理する。ストレージ装置１２０や仮想先ストレージ装置１３０内の構成情報の更新にあわせて、ストレージ管理情報２４２は更新される。その結果、管理計算機１４０とストレージ装置１２０等との間で構成情報が同期する。
【００９９】
管理者認証情報２４３は、管理計算機１４０を使用する管理者を認証するために使用される情報である。
【０１００】
次に、管理者認証情報２４３について説明する。
【０１０１】
図７は、本発明の第１の実施形態の管理者認証情報２４３の一例を示す説明図である。
【０１０２】
管理者認証情報２４３は項目７０１～項目７０３の３つのデータ項目から構成される。
【０１０３】
項目７０１には、管理者を一意に識別するためのユーザＩＤが格納される。
【０１０４】
項目７０２には、管理者のパスワードが格納される。
【０１０５】
項目７０３には、管理者が管理計算機１４０を使って行える操作を制御するロール（役割）情報が格納される。例えばアカウント管理者のロールを持つ管理者は、管理計算機１４０内のアカウント情報の作成及び削除等をすることができる。セキュリティ管理者のロールを持つ管理者は、ストレージ装置１２０への暗号設定操作、及び、管理計算機１４０内の暗号鍵・暗号設定情報バックアップ情報２４１の管理等をすることができる。例えば、後述する暗号鍵・暗号設定情報のバックアップ及びリストアの指示をすることは、セキュリティ管理者のロールを持つ管理者のみに許可される。
【０１０６】

次に管理計算機１４０のプログラム情報について説明する。管理計算機１４０のプログラム情報は、暗号設定指示プログラム２４４、暗号鍵・暗号設定情報バックアップ指示プログラム２４５、暗号鍵・暗号設定情報リストア指示プログラム２４６、ストレージ管理指示プログラム２４７及びアクセス制御プログラム２４８の５つのプログラムから構成される。これらのプログラムは、ＣＰＵ１４１によって実行される。したがって、以下の説明においてこれらのプログラムが実行する処理は、実際にはＣＰＵ１４１によって実行される。

【０１０７】

暗号設定指示プログラム２４４は、ストレージ装置１２０に対して記憶領域の暗号化等、暗号設定を指示する。

【０１０８】

暗号鍵・暗号設定情報バックアップ指示プログラム２４５は、ストレージ装置１２０に対して暗号鍵及び暗号設定情報のバックアップを指示する。

【０１０９】

暗号鍵・暗号設定情報リストア指示プログラム２４６は、管理計算機１４０内の暗号鍵・暗号設定情報バックアップ情報２４１をストレージ装置１２０に対し送信し、暗号鍵及び暗号設定情報のリストアを指示する。

【０１１０】

ストレージ管理指示プログラム２４７は、ストレージ装置１２０及び仮想先ストレージ装置１３０に対して、暗号設定以外の機能、例えば計算機とのパスの設定等、の実行を指示する。

【０１１１】

アクセス制御プログラム２４８は、管理計算機１４０を使用する管理者を管理者認証情報２４３に基づいて認証し、管理者が要求する管理操作の実行を許可又は禁止する。

【０１１２】

以上が本実施例でのストレージ装置１２０、仮想先ストレージ装置１３０及び管理計算機１４０のソフトウェア構成である。

【０１１３】

以下、上記のソフトウェア構成に基づいて本実施形態における暗号鍵・暗号設定情報のバックアップからリストアまでの一連の処理の詳細について説明する。これらの一連の処理は、以下の五つの処理を含む。第１に、ストレージ装置１２０において暗号鍵の生成及び記憶領域の暗号設定の処理が実行される。第２に、管理計算機１４０がストレージ装置１２０に暗号鍵・暗号設定情報のバックアップを指示する。第３に、指示を受けたストレージ装置１２０は暗号鍵・暗号設定情報を管理計算機１４０へバックアップする。第４に、管理計算機１４０からリストア先ストレージ装置に上記のバックアップした情報を送り、リストアを指示する。第５に、リストア指示を受けたストレージ装置がバックアップ情報のリストア可否を判定してリストアする。以下これらの処理の詳細を説明する。

【０１１４】

＜ストレージ装置の暗号設定処理＞

図９は、本発明の第１の実施形態のストレージ装置１２０の暗号設定プログラム２０６が実行する暗号設定処理の一例を示すフローチャートである。

【０１１５】

ストレージ装置１２０の暗号設定プログラム２０６は、管理計算機１４０からストレージ装置１２０又は仮想先ストレージ装置１３０の記憶領域の暗号化要求を受信する（ステップ９０１）。

【０１１６】

次に、暗号設定プログラム２０６は、既にその記憶領域に適用される暗号鍵を生成済みか否かを判定する（ステップ９０２）。例えば、暗号設定プログラム２０６は、暗号化要求によって指定された記憶領域に対応する項目３０７の情報を参照し、鍵ＩＤが格納されていない場合、暗号鍵がまだ生成されていないと判定する。

【０１１７】
暗号鍵がまだ生成されていない場合、暗号設定プログラム２０６は新規暗号鍵を生成し、生成された暗号鍵を暗号鍵管理情報２０４に追加する。以降、指定された記憶領域のデータを、生成された暗号鍵を用いて暗号化・復号化する（ステップ９０３）。
【０１１８】
暗号鍵が生成済みである場合、暗号設定プログラム２０６は既に生成されている暗号鍵を用いて、指定された記憶領域１２５のデータを暗号化・復号化する（ステップ９０４）。この暗号化・復号化の手順は、ステップ９０３と同様である。なお、本フローチャートでは記憶領域ごとに暗号鍵が設定されるが、ストレージ装置ごとに暗号鍵が設定されてもよい。例えば、ストレージ装置１２０の記憶領域１２５の暗号化に使用される鍵一個と、仮想先ストレージ装置１３０の記憶領域１３５の暗号化に使用される鍵一個の計二個の鍵を設定するフローチャートが使用されてもよい。
【０１１９】
ステップ９０３及びステップ９０４に示すように、記憶領域１２５に暗号鍵が設定された後、ストレージ装置１２０のＩ／Ｏ処理プログラム２０５は、その記憶領域１２５へのデータの書き込み要求を受信すると、そのデータを、設定された暗号鍵を用いて暗号化してその記憶領域１２５に書き込む。記憶領域１２５からデータを読み出す要求を受信すると、Ｉ／Ｏ処理プログラム２０５は、要求されたデータを読み出し、設定された暗号鍵を用いてそのデータを復号化して、要求元に送信する。
【０１２０】
記憶領域１２５が記憶領域１３５を仮想化する仮想記憶領域である場合、データ書き込み要求を受信したＩ／Ｏ処理プログラム２０５は、データを暗号化し、その暗号化されたデータを書き込む要求を仮想先ストレージ装置１３０に送信する。仮想先ストレージ装置１３０は、受信したデータを仮想先記憶領域１３５に格納する。データ読み出し要求を受信したＩ／Ｏ処理プログラム２０５は、仮想先ストレージ装置１３０の仮想先記憶領域１３５から暗号化されたデータを読み出し、そのデータを復号化して要求元に送信する。
【０１２１】
記憶領域１２５又は記憶領域１３５に対応する物理的なディスク装置（例えばＨＤＤ）が不正に持ち出され、図示しない他のストレージ装置に接続された場合、その他のストレージ装置はそのＨＤＤに格納されたデータを復号化するために必要な暗号鍵を持たないため、そのＨＤＤに格納されたデータを利用することができない。このようにして、データの不正な持ち出しが防止される。
【０１２２】
しかし、ストレージ装置１２０に発生した故障によって、ストレージ装置１２０が保持する暗号鍵又は暗号設定情報が失われる場合がある。ここで、故障とは、ハードウェアの故障や暗号鍵や暗号設定情報を格納するメモリの揮発、ソフトウェアの故障又はユーザの誤操作等である。この場合、ストレージ装置１２０も記憶領域１２５に格納されたデータを利用できなくなる。ストレージ装置１２０が仮想先ストレージ装置１３０内の記憶領域１３５を仮想化している場合、仮想先ストレージ装置１３０が故障していないにもかかわらず、記憶領域１３５に格納されたデータまでもが利用できなくなる。
【０１２３】
このような場合にもデータを利用できるように、本実施形態では、暗号鍵及び暗号設定情報が管理計算機１４０によってバックアップされる。そして、ストレージ装置１２０に故障が発生した場合、バックアップされている暗号鍵及び暗号設定情報が適切なストレージ装置１２０にリストアされる。以下、このようなバックアップ及びリストアの処理について説明する。
【０１２４】
＜管理計算機によるバックアップ指示処理＞
図１０は、本発明の第１の実施形態の管理計算機１４０の暗号鍵・暗号設定情報バックアップ指示プログラム２４５が実行する暗号鍵・暗号設定情報のバックアップ処理の一例

を示すフローチャートである。

【０１２５】

管理計算機１４０の暗号鍵・暗号設定情報バックアップ指示プログラム２４５は、管理者から暗号鍵・暗号設定情報のバックアップ要求を受信（ステップ１００１）すると、管理者認証情報２４３に基づいて管理者を認証する（ステップ１００２、ステップ１００３）。具体的には、暗号鍵・暗号設定情報バックアップ指示プログラム２４５は、管理者から受信したユーザＩＤ及びパスワードが、管理者認証情報２４３のいずれか一つのエントリの項目７０１及び項目７０２に登録されており、かつ、そのエントリの項目７０３が「セキュリティ管理者」である場合、管理者認証に成功したと判定する。

【０１２６】

管理者認証失敗の場合は処理を終了する。

【０１２７】

一方、管理者認証成功の場合、管理者は管理計算機１４０からストレージ装置１２０に対して、暗号鍵・暗号設定情報のバックアップを指示する（ステップ１００４）。例えば管理者は、ストレージ装置１２０の故障前のいずれかの時点（例えば暗号鍵が生成された時点又は暗号設定が変更された時点等）でバックアップを指示する。この指示を受信したストレージ装置１２０は、暗号鍵・暗号設定情報バックアップ情報２４１を管理計算機１４０に送信する。この処理及び暗号鍵・暗号設定情報バックアップ情報２４１については後述する（図１１及び図８参照）。

【０１２８】

管理計算機１４０は、ストレージ装置１２０から暗号鍵・暗号設定情報バックアップ情報２４１を受信すると、受信した情報を管理計算機１４０のメモリ１４２又は管理計算機１４０の図示しない磁気ディスク装置（ＨＤＤ）等の不揮発記録媒体に格納する（ステップ１００５）。

【０１２９】

＜ストレージ装置でのバックアップ処理＞

図１１は、本発明の第１の実施形態のストレージ装置１２０の暗号鍵・暗号設定情報バックアッププログラム２０７が実行する暗号鍵・暗号設定情報のバックアップ処理の一例を示すフローチャートである。

【０１３０】

ストレージ装置１２０の暗号鍵・暗号設定情報バックアッププログラム２０７は、管理計算機１４０からの暗号鍵・暗号設定情報のバックアップ要求を受信すると（ステップ１１０１）、暗号鍵・暗号設定情報バックアップ情報２４１を生成し、これを管理計算機１４０に送信する（ステップ１１０２）。なお、暗号鍵・暗号設定情報のバックアップは、管理計算機１４０からの指示を受けていない場合に実行されてもよい。例えば、暗号鍵又は暗号設定がストレージ装置１２０で変更されたときに、予め指定された場所に暗号鍵・暗号設定情報バックアッププログラム２０７が自動でバックアップしてもよい。

【０１３１】

図８は、本発明の第１の実施形態の暗号鍵・暗号設定情報バックアップ情報２４１の一例を示す説明図である。

【０１３２】

暗号鍵・暗号設定情報バックアップ情報２４１は、大データ項目８０１及び８１０の２つの情報から構成される。

【０１３３】

大データ項目８０１は、ＬＵ管理情報２０１及び仮想ＬＵマッピング情報２０２の複製情報である。

【０１３４】

大データ項目８１０は、暗号鍵管理情報２０４のバックアップ情報であり、項目８１１～項目８１９の９つのデータ項目から構成される。

【０１３５】

項目８１１には、バックアップ元ストレージ装置１２０の機種・製造番号が格納される。ここで、バックアップ元ストレージ装置１２０とは、大データ項目８０１及び後述する項目８１２～項目８１９の複製元であるストレージ装置１２０を意味する。

【０１３６】

残りの項目８１２～項目８１９は、それぞれ、暗号鍵管理情報２０４の項目６０１～項目６０８の複製情報であるため説明は省略する。なお、項目８１１及び項目８１７には、計算機システムにおいてバックアップ元ストレージ装置１２０及び仮想先ストレージ装置１３０を一意に識別できる値であるかぎり、装置機種・製造番号以外の値が格納されてもよい。

【０１３７】

＜管理計算機によるリストア指示処理＞

図１２は、本発明の第１の実施形態の管理計算機１４０の暗号鍵・暗号設定情報リストア指示プログラム２４６がストレージ装置１２０又は仮想先ストレージ装置１３０に対して実行するリストア指示処理の一例を示すフローチャートである。

【０１３８】

図１２に示す手順は、ストレージ装置１２０が故障したために、ストレージ装置１２０が保持していた暗号鍵・暗号設定情報が失われた場合に、管理計算機１４０にバックアップされていた暗号鍵・暗号設定情報を用いてリストアする処理の例である。

【０１３９】

ここで、本実施形態におけるリストアの類型について説明する。

【０１４０】

ここでは例として、図１においてストレージ装置１２０Ａが仮想先ストレージ装置１３０を仮想化している場合を仮定する。ストレージ装置１２０Ａは複数の記憶領域１２５を備え、それらのうち少なくとも一つは実記憶領域であり、残りは記憶領域１３５を仮想化する仮想記憶領域である。すなわち、仮想記憶領域に書き込まれたデータは、実際には記憶領域１３５に格納される。この場合、ストレージ装置１２０Ａは、自身が備える実記憶領域に使用される暗号鍵及び暗号設定情報（ここではこれらを暗号鍵等と記載する）、及び、自身が備える仮想記憶領域の暗号鍵等を保持している。

【０１４１】

ストレージ装置１２０Ａが故障すると、ストレージ装置１２０Ａが保持していた暗号鍵等が失われる。このため、管理計算機１４０にバックアップされていた暗号鍵等をいずれかの装置にリストアする必要がある。

【０１４２】

まず、ストレージ装置１２０Ａが故障からまだ回復していない場合における、仮想記憶領域に使用される暗号鍵等のリストアについて説明する。

【０１４３】

ストレージ装置１２０Ａが故障からまだ回復していない場合であっても、仮想記憶領域に格納されたデータは実際には記憶領域１３５に格納されている。このため、仮想先ストレージ装置１３０を新たにストレージ装置１２０Ｂに外部接続する（すなわち、ストレージ装置１２０Ｂが新たに仮想先ストレージ装置１３０を仮想化する）ことによって、計算機１００は仮想記憶領域に格納されていたデータにアクセスすることができる。あるいは、計算機１００は、ストレージ装置１２０Ｂを介さずに仮想先ストレージ装置１３０にアクセスしてもよい。

【０１４４】

このため、管理者は、仮想記憶領域に使用される暗号鍵等のリストア先としてストレージ装置１２０Ｂを指定してもよいし、仮想先ストレージ装置１３０自体を指定してもよい。

【０１４５】

リストア先としてストレージ装置１２０Ｂが指定された場合、仮想記憶領域に設定されていた暗号鍵等がストレージ装置１２０Ｂにリストアされる。そして、ストレージ装置１

２０Ａに代わって、ストレージ装置１２０Ｂが仮想先ストレージ装置１３０を仮想化する。ストレージ装置１２０Ｂは、リストアされた暗号鍵を用いて、記憶領域１３５から読み出されたデータを正しく復号化することができる。

【０１４６】

一方、リストア先として仮想先ストレージ装置１３０自体が指定された場合、仮想記憶領域に設定されていた暗号鍵等が仮想先ストレージ装置１３０にリストアされる。この場合、仮想先ストレージ装置１３０は、もはや他のストレージ装置１２０によって仮想化されない。すなわち、仮想先ストレージ装置１３０は、記憶領域１３５へのデータの読み書き要求を計算機１００からストレージ装置１２０を経由せずに受信し、その要求を処理する。このとき、仮想先ストレージ装置１３０は、リストアされた暗号鍵を用いて、記憶領域１３５から読み出されたデータを正しく復号化して計算機１００に応答することができる。

【０１４７】

ただし、このように仮想先ストレージ装置１３０がストレージ装置１２０を経由しないアクセス要求を処理するためには、データを暗号化・復号化する機能及び暗号鍵を管理する機能を仮想先ストレージ装置１３０が備える必要がある。具体的には、仮想先ストレージ装置１３０は、少なくとも暗号鍵管理情報２０４、暗号設定プログラム２０６、暗号鍵・暗号設定情報バックアッププログラム２０７及び暗号鍵・暗号設定情報リストアプログラム２０８と同等の情報及びプログラムを保持する必要がある。さらに、Ｉ／Ｏ処理プログラム２２３は、暗号化及び復号化を実行する機能を備える必要がある。

【０１４８】

次に、ストレージ装置１２０Ａが故障からまだ回復していない場合における、実記憶領域に使用される暗号鍵等のリストアについて説明する。

【０１４９】

ストレージ装置１２０Ａが故障しても、ストレージ装置１２０Ａのディスク装置に保持されているデータが失われていなければ、そのディスク装置をストレージ装置１２０Ｂ又は仮想先ストレージ装置１３０に接続することによって、そのディスク装置に格納されたデータ（すなわち、そのディスク装置に対応する実記憶領域に格納されたデータ）にアクセスすることができる。この場合、ディスク装置をストレージ装置１２０Ｂ又は仮想先ストレージ装置１３０に接続した後で、上記の仮想記憶装置の暗号鍵等のリストアと同様のリストアを実行することによって、そのディスク装置に格納されたデータを正しく復号化することができる。

【０１５０】

次に、ストレージ装置１２０Ａが既に故障から回復している場合における暗号鍵等のリストアについて説明する。

【０１５１】

ストレージ装置１２０Ａから失われた暗号鍵等をリストアする時点で、既にストレージ装置１２０Ａが故障から回復している場合がある。例えば、ストレージ装置１２０Ａの再起動、一時的な故障又はユーザによる誤操作等によって暗号鍵等が失われた場合がこれに相当する。この場合、管理者は、上記のように、ストレージ装置１２０Ｂ又は仮想先ストレージ装置１３０を暗号鍵等のリストア先として指定するのではなく、回復したストレージ装置１２０Ａ自身をリストア先として指定することができる。その結果、失われた暗号鍵等が、それを本来保持していた（すなわちバックアップ元である）ストレージ装置１２０Ａにリストアされる。

【０１５２】

上記の各場合の処理について、以下、詳細に説明する。

【０１５３】

なお、本実施例では管理計算機１４０が行うリストア指示手順として、３通りのリストア指示手順を示す。最初に図１２のリストア指示手順を示す。その他の図１５及び図１６に示すリストア指示手順については、変形例として本実施例の最後に説明する。

【０１５４】
管理計算機１４０の暗号鍵・暗号設定情報リストア指示プログラム２４６は、管理者からのリストア要求を受信する（ステップ１２０１）。
【０１５５】
次に、暗号鍵・暗号設定情報リストア指示プログラム２４６はリストア要求を行った管理者を認証し（ステップ１２０２）、認証成功か否かを判定する（ステップ１２０３）。この認証及び判定は、図１０のステップ１００２及びステップ１００３と同様に実行されてもよい。
【０１５６】
認証失敗の場合は処理を終了する。一方、認証成功の場合、管理者は管理計算機１４０に対し、故障したストレージ装置（以降、故障装置とも呼ぶ）を指定し、当該故障装置の暗号鍵・暗号設定情報バックアップ情報２４１の読み込みを指示する（ステップ１２０４）。
【０１５７】
次に、管理者は、管理計算機１４０に読み込まれた情報に基づいて、故障装置がどの仮想先ストレージ装置１３０を仮想化していたかを確認し（ステップ１２０５）、故障装置が仮想先ストレージ装置１３０を仮想化していたか否かを判定する（ステップ１２０６）。例えば、暗号鍵・暗号設定情報バックアップ情報２４１に含まれる項目４０３のデータを参照することで、故障装置がどの仮想先ストレージ装置１３０を仮想化していたかを判定することができる。
【０１５８】
故障装置が仮想先ストレージ装置１３０を仮想化していなかった場合、管理者は、仮想先ストレージ装置１３０でなく故障装置自身の暗号鍵・暗号設定情報をリストアするか否かを判定する（ステップ１２０７）。
【０１５９】
故障装置自身の暗号鍵・暗号設定情報をリストアする場合、管理者は、リストア先ストレージ装置（以下、リストア先装置とも呼ぶ）を決める。リストア先とは、バックアップされていた暗号鍵・暗号設定情報をリストアのためにコピーするときのコピー先を意味する。例えば、図１のストレージ装置１２０Ａに故障が発生した場合、故障していないストレージ装置１２０Ｂがリストア先装置に決定されてもよい。そして、管理者は、リストア先装置をシステムオプションモードに設定してから故障装置の暗号鍵・暗号設定情報バックアップ情報２４１をリストア先装置に送り、リストアを指示する（ステップ１２０８）。
【０１６０】
ここで、システムオプションモードについて説明する。
【０１６１】
システムオプションモードに設定されたストレージ装置１２０では、暗号鍵・暗号設定情報バックアップ情報２４１内のバックアップ元装置番号が自装置番号と異なっている場合、及び、暗号鍵が既にストレージ装置１２０に設定済みである場合にも、暗号鍵・暗号設定情報のリストアが許可される。
【０１６２】
通常（すなわち、システムオプションモードに設定されていない場合）、ストレージ装置１２０からバックアップした暗号鍵のうち、仮想先ストレージ装置１３０用の暗号鍵はリストア先装置にリストアできる。しかし、ストレージ装置１２０用の暗号鍵のリストアは、その暗号鍵のバックアップ元装置とリストア先装置とが同一でない限り、実行できない。これは、リストア先ストレージ装置１２０に設定されていた暗号鍵に、別の暗号鍵がリストアによって上書きされる結果、そのストレージ装置１２０がリストア前から保持していた記憶領域１２５のデータが利用できなくなることを防ぐためである。
【０１６３】
しかし、ストレージ装置１２０が故障しても、データを保存するディスク装置は故障し

ていない場合がある。その場合、例えば故障装置のディスク装置をリストア先装置に移して、バックアップされた故障装置の暗号鍵をリストア先装置にリストアすることによって、ディスク装置内の暗号データを復号できるようになる。

【０１６４】

あるいは、ストレージ装置１２０は故障していないが、ストレージ装置１２０内の暗号鍵が壊れてしまった場合（例えば、誤って消去された場合等）、壊れた暗号鍵を、バックアップしてある壊れてない暗号鍵で上書きすることによって、ストレージ装置１２０の暗号データを復号できるようになる。

【０１６５】

システムオプションモードは、例えば上記のような目的で暗号鍵の上書きを許可するために設定される。したがって、上記のような場合以外には、通常、システムオプションモードを設定しなくてもよい。

【０１６６】

次に、リストア先装置は故障装置の暗号鍵・暗号設定情報バックアップ情報２４１を受信し、リストアを実行し、リストア終了を管理計算機１４０に通知する（ステップ１２０９）。具体的には、このリストアによって、リストア先装置のＬＵ管理情報２０１、ＬＵマッピング情報２０２及び暗号鍵管理情報２０４が、暗号鍵・暗号設定情報バックアップ情報２４１に含まれるデータによって上書きされる。

【０１６７】

管理者は、リストア先装置でのリストア終了後、故障装置の暗号鍵・暗号設定情報バックアップ情報２４１を参照し、故障装置の記憶領域と計算機１００との間に設定されていたパス（すなわち通信可能な経路）を参考に、リストア先装置の記憶領域と計算機１００間のパスを設定する（ステップ１２１０）。

【０１６８】

例えば、故障装置が、ＬＵ番号「３」に対応するＬＵ（項目３０２参照）と、ＷＷＮ「２０：００：００：００：００：００：Ａ１：７Ａ」によって識別される計算機１００（項目３０４参照）との間にパスを設定していた場合、管理者は、当該ＬＵに対応するリストア先装置のＬＵ１２５（すなわち、故障装置が仮想化していたＬＵ１３５と同じ仮想先ストレージ装置１３０のＬＵ１３５を仮想化するＬＵ１２５）と、ＷＷＮ「２０：００：００：００：００：００：Ａ１：７Ａ」によって識別される計算機１００との間にパスを設定する。

【０１６９】

具体的には、リストア先装置のＬＵ管理情報２０１の項目３０２の値「３」に対応する項目３０４に「２０：００：００：００：００：００：Ａ１：７Ａ」が格納される。この設定は、リストア先装置が、「２０：００：００：００：００：００：Ａ１：７Ａ」によって識別される計算機１００による、ＬＵ「３」へのアクセスを許可することを意味する。

【０１７０】

但し、故障等を契機に従来とは異なるパスが設定されてもよい。またステップ１２１０の処理を管理者ではなく、リストア先装置自身が、管理計算機１４０から受信した故障装置の暗号鍵・暗号設定情報バックアップ情報２４１を参照して、実行してもよい。

【０１７１】

ステップ１２０７で故障装置自身の暗号鍵・暗号設定情報をリストアしない場合は処理を終了する。

【０１７２】

ステップ１２０６で、故障装置が仮想先ストレージ装置１３０を仮想化していた場合、管理者は、故障装置によって仮想化されていたその仮想先ストレージ装置１３０内の記憶領域のＬＵＮ　Ｓｅｃｕｒｉｔｙの設定を解除する（ステップ１２１１）。その結果、他のストレージ装置１２０がその仮想先ストレージ装置１３０にアクセスできるようになる。例えば項目３０４では、ストレージ装置１２０の各ＬＵへアクセス可能な計算機１００

が制限されている。仮想先ストレージ装置１３０においても同様のアクセス制限が設定されていると考える。但し、ステップ１２１１は必須の処理ではなく、当該仮想先ストレージ装置１３０内の記憶領域にＬＵＮ　Ｓｅｃｕｒｉｔｙがもともと設定されていないのであれば実行する必要はない。

【０１７３】

次に管理者は、暗号鍵・暗号設定情報バックアップ情報２４１の中から、故障装置からバックアップされた情報を選択し、リストアされる仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を指定し（言い換えると、選択された情報の中の、どの仮想先ストレージ装置１３０の暗号鍵・暗号設定情報をリストアするかを指定し）、さらに、その暗号鍵・暗号設定情報がリストアされるリストア先装置を指定し、リストアを要求する（ステップ１２１２）。

【０１７４】

管理計算機１４０は、複数の仮想先ストレージ装置１３０を仮想化するストレージ装置１２０の暗号鍵・暗号設定情報をバックアップするとき、自装置及び複数の仮想先ストレージ装置１３０全ての暗号鍵・暗号設定情報を一つのファイルとしてバックアップしてもよいし、仮想先ストレージ装置１３０ごとに暗号鍵・暗号設定情報を一つのファイルとしてバックアップしてもよい。後者の場合は暗号鍵・暗号設定情報は複数になる。この場合、ステップ１２１２において、複数の暗号鍵・暗号設定情報バックアップ情報２４１の中から、故障装置からバックアップされた情報が選択される。

【０１７５】

また、例えば図８の暗号鍵・暗号設定情報バックアップ情報２４１の場合、項目８１７に登録された装置のうち、「Ｄ６００－１００」だけを管理者が指定した場合、その番号が示す仮想先ストレージ装置１３０の暗号鍵及び暗号設定情報（すなわち、鍵ＩＤ「２」から「４」に対応する項目８１３、８１４及び８１５等の情報）のみのリストアが要求され、「Ｄ７００－１１０」に対応する暗号鍵及び暗号設定情報はリストア要求されない。一方、「Ｄ６００－１００」及び「Ｄ７００－１１０」が指定された場合、鍵ＩＤ「２」から「５」に対応する暗号鍵及び暗号設定情報のリストアが要求される。

【０１７６】

次に、管理計算機１４０は、ステップ１２１２において管理者が指定した一つ以上の仮想先ストレージ装置１３０が、リストア先装置と同じ装置を含むか否かを判定する（ステップ１２１３）。即ち、故障装置によって仮想化されていた仮想先ストレージ装置１３０の暗号鍵及び暗号設定情報が、その仮想先ストレージ装置１３０自体へリストアされるか否かが判定される。

【０１７７】

例えば、ステップ１２１２において、仮想先ストレージ装置「Ｄ６００－１００」及び「Ｄ７００－１１０」の暗号鍵及び暗号設定情報が、仮想先ストレージ装置「Ｄ６００－１００」にリストアされることが指定された場合、ステップ１２１３において、故障装置によって仮想化されていた仮想先ストレージ装置１３０（すなわち「Ｄ６００－１００」）の暗号鍵及び暗号設定情報が、その仮想先ストレージ装置１３０自体へリストアされると判定される。

【０１７８】

管理者が指定した一つ以上の仮想先ストレージ装置１３０がリストア先装置と同じ装置を含まない場合、管理計算機１４０は、指定された仮想先ストレージ装置１３０をリストア先装置に外部接続し、指定された仮想先ストレージ装置１３０のＬＵ１３５を仮想化する（ステップ１２１４）。言い換えると、指定された仮想先ストレージ装置１３０の記憶領域１３５は、リストア先装置によって仮想化される。例えば管理計算機１４０は、項目４０４の情報に基づいて、仮想先ストレージ装置１３０を外部接続する。

【０１７９】

次に、管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１のうち、管理者が指定した仮想先ストレージ装置１３０の暗号鍵・暗号設定情報だ

けをリストア先装置へ送信し、リストアを指示する（ステップ１２１５）。

【０１８０】

リストア先装置は、管理計算機１４０から仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を受信すると、リストア処理を実行する。具体的には、リストア先装置は、受信した暗号鍵・暗号設定情報をリストア可能か否かを判定する。リストア可能な場合、リストア先装置は、受信した暗号鍵・暗号設定情報をそのリストア先装置が保持するＬＵ管理情報２０１、仮想ＬＵマッピング情報２０２及び暗号鍵管理情報２０４に追加する。そして、リストア先装置は、リストア結果を管理計算機１４０に通知する（ステップ１２１６）。なお、ストレージ装置１３０でのリストア処理の詳細については後述する。

【０１８１】

次に、管理者は、故障装置の暗号鍵・暗号設定情報バックアップ情報２４１を参照し、故障装置の仮想ＬＵ（仮想先ストレージ装置１３０のＬＵを仮想化したＬＵ）のうちリストアされたものについて、当該ＬＵと計算機１００間に設定されていたパスを参考に、リストア先装置の仮想ＬＵ（ステップ１２１４で仮想化したＬＵ）と計算機１００との間のパスを設定する（ステップ１２１７）。

【０１８２】

例えば、図１において、仮想先ストレージ装置１３０を仮想化しているストレージ装置１２０Ａが故障し、ストレージ装置１２０Ａの記憶領域１２５に設定されていた暗号鍵等がストレージ装置１２０Ｂにリストアされた場合、管理者は、リストア先のストレージ装置１２０Ｂの仮想記憶領域（図示省略）と、計算機１００との間にパスを設定する。この設定は、ストレージ装置１２０Ｂが、計算機１００によるストレージ装置１２０Ｂの仮想記憶領域へのアクセスを許可することを意味する。このパスの設定は、例えばステップ１２１０と同様の方法によって実行される。

【０１８３】

ステップ１２１３において、管理者が指定した一つ以上の仮想先ストレージ装置１３０が、リストア先装置と同じ装置を含む場合、そのリストア先装置と同じ装置の暗号鍵・暗号設定情報をリストアするために、処理はステップ１２１８に進み、リストア先装置と異なる装置の暗号鍵・暗号設定情報をリストアするために、処理はステップ１２１４に進む（ステップ１２１８）。

【０１８４】

ステップ１２１４～１２１７の処理については既に説明したため、ステップ１２１８以降の処理について以下に説明する。

【０１８５】

管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０（すなわちリストア先装置）の仮想ＬＵを、リストア先装置の実ＬＵとしてマッピングする（ステップ１２１９）。

【０１８６】

例えば、項目４０２のＬＵ番号「３」に対応するＬＵは、故障装置が仮想先ストレージ装置１３０内のＬＵ番号「１」のＬＵを仮想化している仮想ＬＵである。このＬＵ番号「３」のＬＵの暗号設定情報（例えば項目３０６及び項目３０７の情報）を、仮想先ストレージ装置１３０自身にリストアする場合について説明する。この場合、管理計算機１４０は、仮想先ストレージ装置１３０に対して自装置内のこのＬＵ番号「１」のＬＵの仮想化は指示しない。その結果、仮想先ストレージ装置１３０は、ＬＵ番号「１」のＬＵを自装置内に実在する実ＬＵとして扱う。具体的には、故障装置が保持するＬＵ管理情報２０１において、ＬＵ番号「３」のＬＵの項目３０５は「仮想」となっている。しかし、そのＬＵ管理情報２０１のバックアップ情報（図８参照）を仮想先ストレージ装置１３０にリストアすると、このＬＵ番号「３」がＬＵ番号「１」に変更され、項目３０５は「実」に変更される。さらに、仮想ＬＵマッピング情報２０２の項目４０２のＬＵ番号「３」に対応して登録されていた仮想ＬＵマッピング情報は削除される。

【０１８７】

次に、管理計算機１４０は、管理者が選択した暗号鍵・暗号設定情報バックアップ情報２４１のうち、管理者が指定した仮想先ストレージ装置１３０の暗号鍵・暗号設定情報だけをリストア先装置へ送信し、リストアを指示する（ステップ１２２０）。

【０１８８】

リストア先装置は、管理計算機１４０から仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を受信すると、リストア実行する。具体的には、リストア先装置は、受信した暗号鍵・暗号設定情報をそのリストア先装置が保持するＬＵ管理情報２０１、仮想ＬＵマッピング情報２０２及び暗号鍵管理情報２０４に追加する。このとき、リストア先装置は、ステップ１２１９において説明したように値を変更する。そして、リストア先装置は、リストア結果を管理計算機１４０に通知する（ステップ１２２１）。

【０１８９】

次に、管理者は、故障装置の暗号鍵・暗号設定情報のバックアップ情報を参照し、故障装置の仮想ＬＵと計算機１００間に設定されていたパスを参考に、リストア先装置でマッピングした実ＬＵと計算機１００間との間にパスを設定する（ステップ１２２２）。

【０１９０】

例えば、図１において、仮想先ストレージ装置１３０を仮想化しているストレージ装置１２０Ａが故障し、ストレージ装置１２０Ａの記憶領域１２５に設定されていた暗号鍵等が仮想先ストレージ装置１３０にリストアされた場合、管理者は、リストア先である仮想先ストレージ装置１３０の記憶領域１３５と、計算機１００との間にパスを設定する。この設定は、仮想先ストレージ装置１３０が、計算機１００による記憶領域１３５へのアクセスを許可することを意味する。このパスの設定は、例えばステップ１２１０と同様の方法によって実行される。

【０１９１】

以上が、管理計算機１４０からリストア先ストレージ装置へのリストア指示処理のフローである。

【０１９２】

なお、ステップ１２１９において、管理計算機１４０は、仮想化されていたリストア先装置自体の暗号鍵及び暗号設定情報については、暗号鍵・暗号設定情報バックアップ情報２４１の送信によるリストア指示とは別に、管理計算機１４０が直接リストア先装置に暗号設定の変更を指示してもよい。

【０１９３】

また、ステップ１２１９において、管理計算機１４０は、リストア先装置自体の暗号鍵及び暗号設定情報については、暗号鍵・暗号設定情報バックアップ情報２４１に基づいて新たな暗号鍵・暗号設定情報バックアップ情報２４１を作成し、その新たな暗号鍵・暗号設定情報バックアップ情報２４１を送信することによってリストアを指示してもよい。その場合、暗号鍵・暗号設定情報バックアップ情報２４１内のバックアップ元装置機種・製造番号（項目８１１）をリストア先装置の装置機種・製造番号とし、当該リストア先装置の項目３０２のＬＵ番号を項目４０５のＬＵ番号で置き換え、当該ＬＵの項目３０５を「仮想」から「実」に置き換えることによって、新たな暗号鍵・暗号設定情報バックアップ情報２４１が作成される。

【０１９４】

なお、リストアに成功した後、仮想先ストレージ装置１３０のＬＵにリストア先装置以外のストレージ装置１２０がアクセスできないように、ＬＵＮ　Ｓｅｃｕｒｉｔｙを設定することによってアクセスを制限してもよい。

【０１９５】

＜ストレージ装置のリストア処理＞

図１３は、本発明の第１の実施形態において管理計算機１４０からリストア指示を受けたストレージ装置が実行するリストア処理の一例を示すフローチャートである。

【０１９６】

既に説明したように、ストレージ装置１２０又は仮想先ストレージ装置１３０がリスト

ア先として指定される。図１３に示す処理は、リストア指示を受信したストレージ装置１２０又は仮想先ストレージ装置１３０によって実行される。図１３の各ステップを実行する「ストレージ装置」は、リストア指示を受信したストレージ装置１２０又は仮想先ストレージ装置１３０である。図１４及び図１７に示す変形例についても同様である。

【０１９７】

ストレージ装置は、管理計算機１４０からリストア指示とともに、故障装置の１以上の暗号鍵・暗号設定情報バックアップ情報２４１を受信（ステップ１３０１）する。ここで受信したリストア指示及び暗号鍵・暗号設定情報バックアップ情報２４１は、図１２のステップ１２０８、ステップ１２１５又はステップ１２２０において送信されたものである。

【０１９８】

次に、ストレージ装置は、自装置がシステムオプションモードであるか否かを判定する（ステップ１３０２）。この判定は、例えば、ストレージ装置機種・製造番号管理情報２０３の項目５０３に基づいて実行される。

【０１９９】

システムオプションモードでない場合、ストレージ装置は、管理計算機１４０から受信した暗号鍵・暗号設定情報バックアップ情報２４１内のバックアップ元装置機種・製造番号（項目８１１）を参照する（ステップ１３０３）。

【０２００】

次に、ストレージ装置は、ステップ１３０３で参照されたバックアップ元装置機種・製造番号が自ストレージ装置の装置機種・製造番号（項目５０１）と同じか否かを判定する（ステップ１３０４）。

【０２０１】

バックアップ元装置機種・製造番号が自ストレージ装置の装置機種・製造番号と同じである場合、ストレージ装置１２０からバックアップされた暗号鍵等を、そのストレージ装置１２０自身にリストアすることが指示されている。この場合、ストレージ装置１２０は、リストア対象に既に暗号鍵が設定されているか否かを判定する（ステップ１３０５）。この判定は、ＬＵ管理情報２０１の項目３０７に基づいて実行される。

【０２０２】

なお、記憶領域（ＬＵ）１２５ごとに暗号鍵が設定される場合、リストア対象とは、リストアされる暗号鍵等が設定される記憶領域１２５である。ストレージ装置ごとに暗号鍵が設定される場合、リストア対象とは、リストアされる暗号鍵等が設定されるストレージ装置１２０又は仮想先ストレージ装置１３０である。

【０２０３】

暗号鍵が既に設定されている場合、ストレージ装置は処理を終了し、管理計算機にリストア終了を通知する（ステップ１３０９）。

【０２０４】

暗号鍵が設定されていない場合、ストレージ装置は、受信した暗号鍵・暗号設定情報バックアップ情報（すなわち、リストア先として指定されたストレージ装置１２０からバックアップされた暗号鍵・暗号設定情報バックアップ情報）の暗号鍵がＬＵごとに設定されているか否かを判定する（ステップ１３０６）。例えば、項目８１８にＬＵ番号が格納されていれば、ＬＵごとに暗号鍵が設定されている。一方、「装置」が格納されていれば、装置ごとに暗号鍵が設定されている。

【０２０５】

ＬＵごとに暗号鍵が設定されていない場合、ストレージ装置は、各装置に対応する暗号鍵と、各装置のＬＵに対応する暗号設定情報とをリストアする（ステップ１３０８）。例えば、暗号鍵が装置ごとに設定されており、かつ、リストア先装置に暗号鍵が設定されていない場合、ストレージ装置は、暗号鍵・暗号設定情報バックアップ情報２４１内にある当該リストア先装置の暗号鍵（項目８１３）と、当該リストア先装置の暗号設定情報とをリストア先装置（すなわち自ストレージ装置）に設定する。当該リストア先装置の暗号設

定情報は、少なくとも、当該リストア先装置の各ＬＵの暗号Ｏｎ／Ｏｆｆ情報（項目３０６）を含む。

【０２０６】

ステップ１３０６で暗号鍵がＬＵごとに設定されている場合は、各装置の各ＬＵの暗号鍵及び暗号設定情報を自ストレージ装置にリストアする（ステップ１３０７）。

【０２０７】

ステップ１３０４でバックアップ元装置機種・製造番号が自ストレージ装置の装置機種・製造番号と異なる場合、ストレージ装置１２０からバックアップされた暗号鍵等を、そのストレージ装置１２０（すなわちバックアップ元装置）以外のストレージ装置にリストアすることが指示されている。この場合、ストレージ装置は、管理計算機１４０から受信した暗号鍵・暗号設定情報バックアップ情報が、バックアップ元装置内の実ＬＵの暗号鍵・暗号設定情報を含むか否かを判定する（ステップ１３１０）。例えば図８の場合、鍵ＩＤ「１」に対応する大データ項目８０１内の項目３０５（すなわちバックアップされたＬＵ管理情報２０１の項目３０５）の値が「実」である。この場合、項目８１２の鍵ＩＤ「１」によって識別される暗号鍵はバックアップ元装置内の実ＬＵの暗号鍵であり、ＬＵ番号「１」によって識別されるＬＵの暗号Ｏｎ／Ｏｆｆ及び鍵ＩＤはバックアップ元装置内の実ＬＵの暗号設定情報である。

【０２０８】

受信した情報にバックアップ元装置内の実ＬＵの暗号鍵・暗号設定情報が含まれる場合、ストレージ装置は、バックアップ元装置の暗号鍵・暗号設定情報のリストアを実行せず、ステップ１３１１に進む（ステップ１３１８）。すなわち、この場合、ステップ１３１１以降の処理において、ストレージ装置は、バックアップ元装置内の実ＬＵの暗号鍵・暗号設定情報のリストアを実行しない。

【０２０９】

ステップ１３１０及びステップ１３１８の結果、実ＬＵに設定された暗号鍵・暗号設定情報が、その情報のバックアップ元であるストレージ装置１２０以外の装置にリストアされることが防止される。

【０２１０】

ステップ１３１０において、受信した情報にバックアップ元装置内の実ＬＵの暗号鍵・暗号設定情報が含まれないと判定された場合、ストレージ装置は、暗号鍵・暗号設定情報バックアップ情報２４１内の仮想先装置機種・製造番号の中に、自ストレージ装置の機種・製造番号又は自ストレージ装置が仮想化している仮想先ストレージ装置１３０の装置機種・製造番号（項目５０４）が含まれるか否かを判定する（ステップ１３１１）。

【０２１１】

自ストレージ装置の機種・製造番号又は自ストレージ装置が仮想化している仮想先ストレージ装置１３０の装置機種・製造番号が含まれない場合、処理はステップ１３０９に進む。

【０２１２】

一方、自ストレージ装置の機種・製造番号又は自ストレージ装置が仮想化している仮想先ストレージ装置１３０の装置機種・製造番号が含まれる場合、ストレージ装置は、ステップ１３１１において「含まれる」と判定された装置機種・製造番号が、自ストレージ装置の機種・製造番号と同じか否かを判定する（ステップ１３１２）。言い換えると、ストレージ装置は、装置機種・製造番号が自ストレージ装置の装置機種・製造番号と同じ仮想先ストレージ装置１３０、又は、装置機種・製造番号が自ストレージ装置が仮想化している仮想先ストレージ装置１３０の装置機種・製造番号と同じ仮想先ストレージ装置１３０について、その仮想先ストレージ装置１３０の機種・製造番号が自ストレージ装置の機種・製造番号と同じか否かを判定する。

【０２１３】

同じであると判定された場合、ストレージ装置は、リストア対象に既に暗号鍵が設定されているか判断する。（ステップ１３１３）。

【０２１４】
暗号鍵が設定されている場合、処理はステップ１３１７に進む。
【０２１５】
一方、暗号鍵が設定されていない場合、ストレージ装置は、受信した暗号鍵・暗号設定情報バックアップ情報の暗号鍵がＬＵごとに設定されているか否かを判定する（ステップ１３１４）。
【０２１６】
暗号鍵がＬＵごとに設定されている場合、ストレージ装置は、仮想先ストレージ装置１３０の各ＬＵの暗号鍵及び各ＬＵの暗号設定情報を自ストレージ装置の実ＬＵの暗号鍵及び暗号設定情報としてリストアし、ステップ１３１７に進む（ステップ１３１５）。即ち、バックアップ元であるストレージ装置が仮想ＬＵに割り当てた暗号鍵及び暗号設定情報が、リストア先である仮想先ストレージ装置１３０では、自装置内の実ＬＵの暗号鍵及び暗号設定情報として割り当てられる。
【０２１７】
ステップ１３１４で暗号鍵がＬＵごとに設定されていないと判定された場合、ストレージ装置は、仮想先ストレージ装置１３０の暗号鍵及び各ＬＵの暗号設定情報を自装置の暗号鍵及び実ＬＵの暗号設定情報としてリストアする（ステップ１３１６）。
【０２１８】
次にストレージ装置は、受信した暗号鍵・暗号設定情報バックアップ情報内の仮想先装置機種・製造番号のうち、自ストレージ装置の機種・製造番号又は自ストレージ装置が仮想化している仮想先ストレージ装置１３０の装置機種・製造番号と同じであり、かつ、まだステップ１３１２以降の処理がされていないものがあるか否かを判定する（１３１７）。
【０２１９】
ステップ１３１７の条件を満たすものがある場合、処理はステップ１３１２に戻り、ない場合、処理はステップ１３０９に進む。
【０２２０】
ステップ１３１２において、当該仮想先ストレージ装置１３０の機種・製造番号が自ストレージ装置の機種・製造番号と同じでない場合、ストレージ装置は、リストア対象に既に暗号鍵が設定されているか否かを判定する（ステップ１３１９）。
【０２２１】
暗号鍵が設定されている場合、処理はステップ１３１７に進み、暗号鍵が設定されていない場合、ストレージ装置は、受信した暗号鍵・暗号設定情報バックアップ情報の暗号鍵がＬＵごとに設定されているか否かを判定する（ステップ１３２０）。
【０２２２】
ＬＵごとに設定されている場合、ストレージ装置は、仮想先ストレージ装置１３０の各ＬＵの暗号鍵及び各ＬＵの暗号設定情報を自装置の各仮想ＬＵの暗号鍵及び暗号設定情報としてリストアし、ステップ１３１７に進む（ステップ１３２１）。
【０２２３】
ステップ１３２０において暗号鍵がＬＵごとに設定されていないと判定された場合、ストレージ装置は、仮想先ストレージ装置１３０の暗号鍵及び各ＬＵの暗号設定情報を自装置の暗号鍵及び仮想ＬＵの暗号設定情報としてリストアし、ステップ１３１７に進む（ステップ１３２２）。ステップ１３２１及び１３２２は、ステップ１３１５及び１３１６と同様にして実行される。
【０２２４】
以上が、ストレージ装置によって実行される暗号鍵・暗号設定情報バックアップ情報２４１のリストア処理のフローである。
【０２２５】
尚、上記の図１３の処理は、図１３のリストア処理が実行される前に、リストア先であるストレージ装置１２０が仮想先ストレージ装置１３０のＬＵを仮想化及びマッピングす

る処理が実行されていることが前提となっている。すなわち、先にリストア先ストレージ装置１２０が仮想先装置のＬＵを仮想化及びマッピングしてから、リストア先ストレージ装置１２０が暗号鍵・暗号設定情報バックアップ情報２４１受信する。しかし、必ずしもこの順序でリストアが実行される必要はない。例えば、先に管理計算機１４０がリストア先ストレージ装置１２０に暗号鍵・暗号設定情報バックアップ情報２４１を送信し、その後、リストア先ストレージ装置が仮想先ストレージ装置１３０を仮想化及びマッピングし、それから暗号鍵・暗号設定情報がリストアされてもよい。以下、後者の処理フローを、図１３において説明したストレージ装置のリストア処理フローの変形例として、図１４を用いて説明する。

【０２２６】

＜ストレージ装置のリストア処理の変形例１＞

図１４は、本発明の第１の実施形態において管理計算機１４０からリストア指示を受けたストレージ装置が実行するリストア処理の第１の変形例を示すフローチャートである。

【０２２７】

図１４に示す処理のうち、ステップ１３０１～１３１０及び１３１２～１３２２は、図１３に示すものと同様であるため、説明を省略する。図１４のステップ１３１１において、図１３のステップ１３１１と同様の判定が実行される。しかし、ここで「Ｎｏ」と判定された場合に実行される処理が、図１３と異なる。

【０２２８】

ストレージ装置は、ステップ１３１１において、暗号鍵・暗号設定情報バックアップ情報２４１内の仮想先装置機種・製造番号の中に、自ストレージ装置の機種・製造番号又は自ストレージ装置が仮想化している仮想先ストレージ装置１３０の装置機種・製造番号がないと判定された場合、管理計算機１４０から受信した暗号鍵・暗号設定情報バックアップ情報２４１を、一旦自装置の制御メモリ１２４又はＨＤＤ（図示省略）に保存する。その後、管理者が仮想先ストレージ装置１３０のＬＵを仮想化した後、又は、仮想先ストレージ装置１３０のＬＵを実ＬＵとしてマッピングした後に、保存した暗号鍵・暗号設定情報を上記仮想化又はマッピングされたＬＵに設定する（ステップ１３２３）。

【０２２９】

以上がストレージ装置でのリストア処理の第１の変形例の説明である。

【０２３０】

次に、さらに別の変形例２を図１７を用いて説明する。本変形例では、暗号鍵・暗号設定情報バックアップ情報２４１を受信したストレージ装置１２０が当該バックアップ情報に基づいて自動的に仮想先ストレージ装置１３０を仮想化し、暗号鍵・暗号設定情報をリストアする点が、既に説明したリストア処理と異なる。

【０２３１】

＜ストレージ装置のリストア処理の変形例２＞

図１７は、本発明の第１の実施形態において管理計算機１４０からリストア指示を受けたストレージ装置が実行するリストア処理の第２の変形例を示すフローチャートである。

【０２３２】

第２の変形例では、図１３のステップ１３０１～１３０８、１３１０及び１３１８に示す処理が実行される。これらのステップは図１３において説明したため、図１７では省略されている。

【０２３３】

図１７に示す処理のうち、ステップ１３０９、１３１３～１３１７及び１３２０～１３２２は、図１３に示すものと同様であるため、説明を省略する。

【０２３４】

ステップ１３１０において「Ｎｏ」と判定された場合、及び、ステップ１３１８が実行された場合、ストレージ装置は、ステップ１７０１の判定を実行する。

【０２３５】

図１７のステップ１７０１及び１７０２において、それぞれ、図１３のステップ１３１

１及び１３１２と同様の判定が実行される。しかし、これらのステップで「Ｎｏ」と判定された場合に実行される処理が、図１３と異なる。

【０２３６】

ステップ１７０１において、ストレージ装置は、管理計算機１４０から受信した暗号鍵・暗号設定情報バックアップ情報２４１内の仮想先装置番号の中に、自装置の装置機種・製造番号又は自装置が仮想化している装置の装置機種・製造番号あるか否かを判定する。その結果「Ｎｏ」と判定された場合、処理はステップ１７０３に進む。一方、「Ｙｅｓ」と判定された場合、ストレージ装置は、その装置機種・製造番号が自ストレージ装置の装置機種・製造番号と同じであるか否かを判定する（ステップ１７０２）。

【０２３７】

ステップ１７０２において「Ｙｅｓ」と判定された場合、処理はステップ１３１３に進む。一方、「Ｎｏ」と判定された場合、処理はステップ１７０３に進む。

【０２３８】

ステップ１７０１又はステップ１７０２において「Ｎｏ」と判定された場合、ステップ１７０３において、ストレージ装置１２０は、管理計算機１４０から受信した暗号鍵・暗号設定情報バックアップ情報２４１に含まれる仮想先ストレージ装置１３０のＬＵ１３５を仮想化するために、仮想先ストレージ装置１３０のＬＵ１３５へアクセスを試み（ステップ１７０３）、当該ＬＵ１３５へアクセス可能か否かを判定する（ステップ１７０４）。

【０２３９】

例えば、ストレージ装置１２０がリストア処理を実行する前に項目３０４の設定が解除されていない場合、ストレージ装置１２０は当該ＬＵ１３５へアクセスできない。当該ＬＵ１３５へアクセス不可能であった場合、処理はステップ１３１７へ進む。

【０２４０】

一方、当該ＬＵ１３５へアクセス可能であった場合、ストレージ装置１２０は、自ストレージ装置内に新たな仮想ＬＵ１２５を作成し、当該ＬＵ１３５を仮想化する（ステップ１７０５）。

【０２４１】

例えば、ストレージ装置１２０は仮想化の際に管理者に問い合わせてもよいし、自ストレージ装置内の空いているポートを任意のＬＵにマッピングすることによって仮想化してもよい。

【０２４２】

次に処理はステップ１３２０へ進む。以上がストレージ装置１２０でのリストア処理の第２の変形例の説明である。

【０２４３】

＜管理計算機によるリストア指示処理の変形例１＞

次に管理計算機１４０からのリストア指示フローの第１の変形例を説明する。

【０２４４】

図１５は、本発明の第１の実施形態の管理計算機１４０の暗号鍵・暗号設定情報リストア指示プログラム２４６がストレージ装置１２０又は仮想先ストレージ装置１３０に対して実行するリストア指示処理の第１の変形例を示すフローチャートである。

【０２４５】

図１５の処理のうち、ステップ１２０１～１２１１、１２１６、１２１７、１２２１及び１２２２は、図１２に示すものと同じである。このため、これらのステップについての説明は省略する。

【０２４６】

ステップ１２１１の処理終了後、管理者は、故障装置が仮想化していた仮想先ストレージ装置１３０と、リストア先装置とを選択し、当該仮想先ストレージ装置１３０の暗号鍵・暗号設定情報のリストアを管理計算機に指示する（ステップ１５０１）。

【０２４７】

管理計算機１４０は、指定された仮想先ストレージ装置１３０が暗号化されているか確認する（ステップ１５０２）。

【０２４８】

次に管理計算機１４０は、管理者が指定したリストア先装置と仮想先ストレージ装置１３０とが同じ装置であるか否かを判定する（ステップ１５０３）。

【０２４９】

管理者が指定したリストア先装置と仮想先ストレージ装置１３０とが同じ装置でない場合、管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０をリストア先装置に外部接続し、指定した仮想先ストレージ装置１３０のＬＵ１３５を仮想化する（ステップ１５０４）。例えば、管理者が仮想先ストレージ装置１３０のＬＵ１３５をリストア先装置のどのＬＵ１２５が仮想化するか指定してもよいし、管理計算機１４０がリストア先装置の空いているポートに任意のＬＵを自動的に作成して、作成されたＬＵ１２５とＬＵ１３５とを対応付けてもよい。

【０２５０】

次に管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０が暗号化されているか否かを、管理計算機１４０内の暗号鍵・暗号設定情報バックアップ情報２４１に基づいて判定する（ステップ１５０５）。

【０２５１】

管理者が指定した仮想先ストレージ装置１３０が暗号化されている場合、管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を、管理計算機１４０内の暗号鍵・暗号設定情報バックアップ情報２４１から取得し、取得した情報をリストア先装置へ送信して、リストアを指示する（ステップ１５０６）。

【０２５２】

例えば管理者が指定した仮想先ストレージ装置１３０が項目８１７にない場合、当該仮想先ストレージ装置１３０が暗号化されていないことがわかる。

【０２５３】

一方、例えば図８の例で管理者が指定した仮想先ストレージ装置１３０が「Ｄ７００－１１０」だった場合、その暗号鍵として、項目８１２の鍵ＩＤが「５」である暗号鍵を取得する。

【０２５４】

ステップ１５０５において、管理者が指定した仮想先ストレージ装置１３０が暗号化されていないと判定された場合、管理計算機１４０は暗号鍵・暗号設定情報をリストア先装置に送信せず、処理はステップ１２１７に進む。

【０２５５】

ステップ１５０３において、管理者が指定したリストア先装置と仮想先ストレージ装置１３０とが同じ装置であると判定された場合、管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０のＬＵ１３５を、リストア先装置の実ＬＵとしてマッピングする（ステップ１５０７）。

【０２５６】

次に管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０が暗号化されているか否かを、ステップ１５０５と同様に判定する（ステップ１５０８）。

【０２５７】

管理者が指定した仮想先ストレージ装置１３０が暗号化されている場合、管理計算機１４０は、管理者が指定した仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を、管理計算機１４０内の暗号鍵・暗号設定情報バックアップ情報２４１から取得し、取得した情報をリストア先装置へ送信して、リストアを指示する（ステップ１５０９）。

【０２５８】

ステップ１５０８において、管理者が指定した仮想先ストレージ装置１３０が暗号化されていないと判定された場合、管理計算機１４０は暗号鍵・暗号設定情報をリストア先装置に送らず、処理はステップ１２２２に進む。

【０２５９】
以上が管理計算機１４０からのリストア指示処理の第１の変形例の説明である。
【０２６０】
次に、さらに別の第２の変形例を説明する。上記のリストア指示処理では、管理計算機１４０がストレージ装置１２０の暗号鍵・暗号設定情報バックアップ情報２４１の一部分の取出し等、高度な機能を備えていた。しかし、以下の変形例ではそのような機能が管理計算機１４０になく、管理者は単純にストレージ装置１２０からバックアップした暗号鍵・暗号設定情報バックアップ情報２４１をそのままストレージ装置１２０へリストアする。
【０２６１】
＜管理計算機によるリストア指示処理の変形例２＞
管理計算機１４０からのリストア指示フローの変形例を説明する。
【０２６２】
図１６は、本発明の第１の実施形態の管理計算機１４０の暗号鍵・暗号設定情報リストア指示プログラム２４６がストレージ装置１２０又は仮想先ストレージ装置１３０に対して実行するリストア指示処理の第２の変形例を示すフローチャートである。
【０２６３】
図１６の処理のうち、ステップ１２０１～１２１１、１２１６、１２１７、１２２１及び１２２２は、図１２に示すものと同じである。このため、これらのステップについての説明は省略する。
【０２６４】
ステップ１２１１の処理終了後、管理者はリストア先装置を決定し、さらに、故障装置の仮想先ストレージ装置１３０のうちのどの仮想先ストレージ装置１３０の暗号鍵・暗号設定情報をリストアするかを決定する（ステップ１６０１）。
【０２６５】
管理者は、リストア先装置を仮想先ストレージ装置１３０と同じストレージ装置にしたか否かを判定する（ステップ１６０２）。
【０２６６】
リストア先装置が仮想先ストレージ装置１３０と同じでない場合、管理者は、決定した仮想先ストレージ装置１３０を、管理計算機１４０を使ってリストア先装置に外部接続し、仮想先ストレージ装置１３０のＬＵ１３５を仮想化する（ステップ１６０３）。
【０２６７】
次に管理者は、故障装置の暗号鍵・暗号設定情報バックアップ情報２４１を選択して、選択された情報をそのままリストア先装置に送信し、リストアを指示する（ステップ１６０４）。
【０２６８】
一方、ステップ１６０２において、リストア先装置が仮想先ストレージ装置１３０と同じであると判定された場合、管理者は上記決定した仮想先ストレージ装置１３０の仮想ＬＵを、リストア先装置の実ＬＵとしてマッピングする（ステップ１６０５）。なお、ここでのマッピングとは、管理者が何か特別な操作を行うことを意味するものではなく、当該仮想ＬＵと実ＬＵの実体とが同一のものとみなすことを意味する。
【０２６９】
次に、ステップ１６０４と同様、管理者は故障装置の暗号鍵・暗号設定情報バックアップ情報２４１を選択して、選択された情報をそのままリストア先装置に送信し、リストアを指示する（ステップ１６０６）。
【０２７０】
以上が管理計算機１４０からのリストア指示処理の第２の変形例の説明である。
【０２７１】
次に、本発明の第２の実施形態を説明する。
【０２７２】

第２の実施形態のシステム構成は、第１の実施形態と同じである（図１参照）。このため、システム構成についての説明は省略する。

【０２７３】

第１の実施形態では、故障装置自身又は故障装置が仮想化していた仮想先ストレージ装置１３０の暗号鍵・暗号設定情報がリストアされる。これに対し第２の実施形態では、必ずしも故障してないストレージ装置１２０の暗号鍵・暗号設定情報バックアップ情報２４１を誤って送信する可能性、及び、ストレージ装置１２０のメモリ故障等によって暗号鍵等が失われた場合にバックアップ元ストレージ装置１２０自身に暗号鍵・暗号設定情報バックアップ情報２４１を送信する可能性等も考慮し、管理計算機１４０が暗号鍵・暗号設定情報のリストアを一元的に実行する。

【０２７４】

以下の本実施形態の説明は、ストレージ装置１２０の暗号鍵及び暗号設定情報（図３、図４、図６参照）は暗号設定指示プログラム２４４を用いて設定済みであり、そのバックアップ（図８参照）も取得済みであることを前提とする。また、第１の実施形態と同じ処理については説明を省略する。以下図１８及び図１９を用いて第２の実施形態を説明する。

【０２７５】

本実施形態では、管理計算機１４０は以下の２つの処理を実行する。第１に、ストレージ装置１２０を監視する（図１８参照）。第２に、ストレージ装置１２０の故障が管理者によって確認された後、管理者からのリストア要求を受けると、管理計算機１４０は、管理者が指定したリストア先装置に、管理者が指定した暗号鍵・暗号設定情報バックアップ情報を送信し、リストアを指示する（図１９参照）。

【０２７６】

＜管理計算機によるストレージ装置の監視処理＞

図１８は、本発明の第２の実施形態の管理計算機１４０のストレージ管理指示プログラム２４７が実行するストレージ装置１２０の監視処理の一例を示すフローチャートである。

【０２７７】

管理計算機１４０は、ストレージ装置１２０に定期的に、所定の信号（いわゆるハートビート）を送信し、その信号に対する応答の有無を監視する（ステップ１８０１）。

【０２７８】

管理計算機１４０は、ストレージ装置１２０から上記の応答を受信しなかった場合、そのことを管理者に通知する。例えば、管理計算機は、ストレージ装置１２０にハートビートを送信した後、所定の時間が経過してもそのハートビートに対する応答を受信しなかった場合、ハートビートを受信しなかったことを示すアラートを管理者に通知してもよい。

【０２７９】

管理者は、ストレージ装置の故障有無を確認する（ステップ１８０２）。この確認は、管理者が管理計算機１４０又はストレージ装置１２０の管理端末（図示省略）を介してストレージ装置１２０の状態確認のためのメンテナンス操作を実行する等の方法によって実行されてもよい。

【０２８０】

故障があった場合、管理者はストレージ装置１２０をＦＣスイッチ１１０から取り外す（ステップ１８０３）。

【０２８１】

＜管理計算機によるリストア指示処理＞

図１９は、本発明の第２の実施形態の管理計算機１４０の暗号鍵・暗号設定情報リストア指示プログラム２４６が実行するストレージ装置１２０へのリストア指示処理の一例を示すフローチャートである。

【０２８２】

図１９の処理は、図１８の処理によってストレージ装置１２０が故障していると判定さ

れたときに実行されてもよいし、それ以外の場合に実行されてもよい。

【０２８３】

管理計算機１４０は、管理者から暗号鍵・暗号設定情報のリストア要求を受信（ステップ１９０１）し、管理者を認証する（ステップ１９０２、ステップ１９０３）。この認証は、図１２のステップ１２０２及び１２０３と同様にして実行される。

【０２８４】

管理者認証失敗の場合は処理を終了する。

【０２８５】

管理者認証成功の場合、管理計算機１４０は、管理者からリストア先装置及びリストアされる暗号鍵・暗号設定情報バックアップ情報２４１の指定を受け付ける（ステップ１９０４）。

【０２８６】

次に、管理計算機１４０は、指定された暗号鍵・暗号設定情報バックアップ情報２４１が示すバックアップ元装置が故障しているか否かを判定する（ステップ１９０５）。例えば、管理計算機１４０は、指定された暗号鍵・暗号設定情報バックアップ情報２４１のバックアップ元装置のＩＰアドレスに対してハートビートを送信し、そのハートビートに対する応答の有無を判定してもよい。あるいは、管理計算機１４０は、ディスカバリを実行してもよい。あるいは、管理計算機１４０は、管理計算機１４０内のバックアップ元装置の構成情報有無を確認してもよい。

【０２８７】

バックアップ元装置のＩＰアドレスは、例えば項目５０２又はストレージ管理情報２４２から取得することができる。バックアップ元装置が故障してＦＣスイッチ１１０から取り外されたような場合は、そのバックアップ元装置（すなわち故障装置）の構成情報は管理計算機１４０から削除されるため、当該バックアップ元装置のＩＰを取得できない可能性がある。しかし、バックアップ元装置の構成情報がない場合に、当該バックアップ元装置が計算機システムに存在しない（すなわち故障等のために取り外された）と判定することができる。

【０２８８】

管理計算機１４０は、例えば上記ステップ１９０５に示し方法によって、バックアップ元装置が故障しているか否かを判定する（ステップ１９０６）。

【０２８９】

バックアップ元装置が故障していないと判定された場合、管理計算機１４０は、バックアップ元装置とリストア先装置とが同じであるか否かを判定する（ステップ１９１３）。

【０２９０】

バックアップ元装置とリストア先装置とが同じでない場合、バックアップ元装置が故障していないにもかかわらず、そのバックアップ元装置からバックアップされた暗号鍵等を他の装置にリストアすることを要求されている。本実施形態では、このようなリストアは許可されないため、処理を終了する。

【０２９１】

一方、バックアップ元装置とリストア先装置とが同じである場合、バックアップ元装置からバックアップされた暗号鍵等を、そのバックアップ元装置にリストアすることを要求されている。例えば一時的な故障等によって、バックアップ元装置が暗号鍵等を失った場合に、このような要求がされる場合がある。この場合、管理計算機１４０は、暗号鍵・暗号設定情報バックアップ情報２４１をリストア先装置に送信し、リストアを指示する（ステップ１９１４）。

【０２９２】

次に管理計算機１４０は、リストア先装置の記憶領域と計算機１００との間のパスが設定済みか否かを判定する（ステップ１９１５）。

【０２９３】

パスが設定済みである場合は処理を終了する。

【０２９４】
パスが設定済みでない場合、管理計算機１４０は、リストア先装置からリストア終了の通知を受信するのを待つ。リストア終了の通知を受信すると、管理計算機１４０は、リストア先装置のＬＵと計算機１００との間のパスを設定する（ステップ１９１６）。例えばリストア前と同じパスを設定する場合、管理計算機１４０は、項目３０４の設定と同じようにパスを設定する。
【０２９５】
ステップ１９０６において、バックアップ元装置が故障していると判定された場合、管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１が仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を含んでいるか否かを判定する（ステップ１９０７）。
【０２９６】
管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１が仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を含んでいない場合はステップ１９１４に進む。
【０２９７】
管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１が仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を含んでいる場合、管理計算機１４０は、仮想先ストレージ装置１３０の記憶領域のＬＵＮ　Ｓｅｃｕｒｉｔｙを解除する（ステップ１９０８）。その結果、他のストレージ装置１２０が仮想先ストレージ装置１３０にアクセスできるようになる。但し、ステップ１９０８は必須の処理ではない。当該仮想先ストレージ装置１３０内の記憶領域にＬＵＮ　Ｓｅｃｕｒｉｔｙがもともと設定されていない場合、ステップ１９０８を実行する必要はない。
【０２９８】
次に管理計算機１４０は、リストア先装置が暗号鍵・暗号設定情報バックアップ情報２４１に含まれる仮想先ストレージ装置１３０と同じであるか否かを判定する（ステップ１９０９）。
【０２９９】
リストア先装置が暗号鍵・暗号設定情報バックアップ情報２４１に含まれる仮想先ストレージ装置１３０と同じでない場合、管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１に含まれる仮想先ストレージ装置１３０をリストア先装置に外部接続し、当該仮想先ストレージ装置１３０のＬＵ１３５を仮想化する（ステップ１９１０）。
【０３００】
次に管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１をリストア先装置に送信し、リストアを指示する（ステップ１９１１）。
【０３０１】
管理計算機１４０は、リストア先装置からのリストア終了の通知を受けると、バックアップ元装置の仮想ＬＵとパスを介して通信可能に接続されていた計算機１００と、リストア先装置の仮想ＬＵとの間にパスを設定する（ステップ１９１２）。例えば図４の項目４０２のＬＵ番号「３」によって識別されるＬＵ１２５が仮想化していた、仮想先ストレージ装置１３０内のＬＵ番号「１」によって識別されるＬＵ１３５をリストア先装置が新たに仮想化してリストアする場合、図３でＬＵ番号「３」によって識別されるＬＵに設定されていた項目３０４の計算機と、リストア先装置の新たな仮想化ＬＵとの間にパスを設定する。但し、故障等を契機に、従来とは異なるパスが設定されてもよい。
【０３０２】
次に管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１が、他の仮想先ストレージ装置１３０の暗号鍵・暗号設定情報を含むか否かを判定する（ステップ１９２０）。
【０３０３】
他の仮想先ストレージ装置１３０の暗号鍵・暗号設定情報が含まれる場合、処理はステ

ップ１９０８に進む。
【０３０４】
一方、他の仮想先ストレージ装置１３０の暗号鍵・暗号設定情報が含まれない場合、処理を終了する。
【０３０５】
ステップ１９０９において、リストア先装置が暗号鍵・暗号設定情報バックアップ情報２４１に含まれる仮想先ストレージ装置１３０と同じであると判定された場合、管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１に含まれる仮想先ストレージ装置１３０のＬＵ１３５を仮想化する仮想ＬＵを、リストア先装置の実ＬＵとしてマッピングする（ステップ１９１７）。
【０３０６】
次に管理計算機１４０は、管理者が指定した暗号鍵・暗号設定情報バックアップ情報２４１をリストア先装置に送信し、リストアを指示する（ステップ１９１８）。
【０３０７】
管理計算機１４０は、リストア先装置からのリストア結果の通知を受けると、バックアップ元装置の仮想ＬＵとパスを介して通信可能に接続されていた計算機と、リストア先装置の実ＬＵとの間にパスを設定する（ステップ１９１９）。その後、処理はステップ１９２０に進む。
【０３０８】
次に、本発明の第３の実施形態について説明する。
【０３０９】
図２０は、本発明の第３の実施形態の計算機システムのハードウェア構成を示すブロック図である。
【０３１０】
第３の実施形態では、第１及び第２の実施形態の計算機システム構成に、ストレージ装置１２０の暗号鍵・暗号設定情報を統合管理する暗号管理サーバ１５０が追加されている。
【０３１１】
本実施形態での処理の概要を説明する。
【０３１２】
管理者は、暗号鍵・暗号設定情報をバックアップする場合、ストレージ装置１２０に対して暗号管理サーバ１５０へのバックアップを指示する。指示を受けたストレージ装置１２０は暗号管理サーバ１５０へ暗号鍵・暗号設定情報をバックアップする。一方暗号鍵・暗号設定情報をリストアする場合、管理者は、暗号管理サーバ１５０に対して、暗号管理サーバ１５０内の暗号鍵・暗号設定情報をストレージ装置１２０へ送信するよう指示する。指示を受けた暗号管理サーバ１５０は、暗号鍵・暗号設定情報をストレージ装置１２０に送信する。それを受信したストレージ装置１２０は暗号鍵・暗号設定情報をリストアする。
【０３１３】
暗号管理サーバ１５０について説明する。
【０３１４】
暗号管理サーバ１５０は、ＣＰＵ１５１、メモリ１５２及び管理Ｉ／Ｆ１５３を備える。管理Ｉ／Ｆ１５３は、ＩＰネットワーク経由で計算機１００及び管理計算機１４０と接続される。管理計算機１４０は、管理Ｉ／Ｆ１５３を介して暗号管理サーバ１５０を管理することができる。尚、暗号管理サーバ１５０は、ＦＣネットワーク経由でストレージ装置１２０及び仮想先ストレージ装置１３０と接続されてもよい。
【０３１５】
暗号管理サーバ１５０は、暗号管理サーバ１５０の図示しない磁気ディスク装置等の不揮発記録媒体に記録された、ストレージ装置１２０の暗号鍵・暗号設定情報バックアップ情報２４１の管理のためのプログラム等を、暗号管理サーバ１５０の起動時等にメモリ１

５２にロードする。ＣＰＵ１５１は、それらのロードしたプログラムを実行することで、ストレージ装置１２０への暗号鍵・暗号設定情報バックアップ情報２４１の送信及び受信等を実行することができる。

【０３１６】

次に、本実施形態でのストレージ装置１２０及び暗号管理サーバ１５０のソフトウェア構成について説明する。

【０３１７】

図２１は、本発明の第３の実施形態の計算機システムのソフトウェア構成の一例を示す説明図である。

【０３１８】

暗号管理サーバ１５０のメモリ１５２には、暗号鍵・暗号設定情報バックアップ情報統合管理情報２１０１、管理者認証情報２１０２、暗号鍵・暗号設定情報バックアップ情報統合管理プログラム２１０３及びアクセス制御プログラム２１０４が格納される。

【０３１９】

図２２は、本発明の第３の実施形態の暗号鍵・暗号設定情報バックアップ情報統合管理情報２１０１の一例を示す説明図である。

【０３２０】

暗号鍵・暗号設定情報バックアップ情報統合管理情報２１０１は、項目２２０１～２２０３の３つのデータ項目から構成される。

【０３２１】

項目２２０１には、暗号管理サーバ１５０に暗号鍵・暗号設定情報バックアップ情報を送信するストレージ装置１２０又は仮想先ストレージ装置１３０のＩＰアドレス又はホスト名が格納される。但し本項目の値はこれらに限定されない。ストレージ装置１２０等を一意に識別できる値である限り、例えばストレージ装置１２０等のポート名（ＷＷＮ）等が格納されてもよい。

【０３２２】

項目２２０２には、項目２２０１によって識別されるストレージ装置１２０等からバックアップされた暗号鍵・暗号設定情報バックアップ情報２４１の識別子が格納される。

【０３２３】

項目２２０３には、項目２２０２によって識別されるデータへのアクセスが許可された管理者を識別する情報が格納される。例えば管理者は、項目２２０２によって識別されるデータのうち、その管理者がアクセスを許可されたものを、ストレージ装置１２０等へ送信することを、暗号管理サーバ１５０に指示することができる。

【０３２４】

図２３は、本発明の第３の実施形態の管理者認証情報２１０２の一例を示す説明図である。

【０３２５】

管理者認証情報２１０２は、項目２３０１～２３０３の３つのデータ項目から構成される。

【０３２６】

項目２３０１には、暗号管理サーバを使用する管理者を一意に識別するためのユーザＩＤが格納される。

【０３２７】

項目２３０２には、暗号管理サーバにログインするための管理者のパスワードが格納される。

【０３２８】

項目２３０３には、管理者が暗号管理サーバで実行できる操作を制御するロール情報が格納される。例えば、ユーザＩＤ「ＡＢＣ」に対応するロール情報として「暗号鍵・暗号設定情報バックアップ情報の送信指示」が格納されている場合、ユーザＩＤ「ＡＢＣ」によって識別される管理者は、項目２２０２によって識別されるデータをストレージ装置へ

送信するよう暗号管理サーバ１５０に指示することができる。

【０３２９】

次に、再び図２１を参照して、暗号管理サーバ１５０のプログラム情報について説明する。メモリ１５２には、暗号鍵・暗号設定情報バックアップ情報統合管理プログラム２１０３及びアクセス制御プログラム２１０４が格納される。

【０３３０】

暗号鍵・暗号設定情報バックアップ情報統合管理プログラム２１０３は、管理者からの指示を受けて項目２２０２のデータをストレージ装置１２０等へ送信する。さらに、暗号鍵・暗号設定情報バックアップ情報統合管理プログラム２１０３は、ストレージ装置１２０等から受信した暗号鍵・暗号設定情報バックアップ情報を、各ストレージ装置１２０等に対応付けて図２２のような形で管理する。

【０３３１】

アクセス制御プログラム２１０４は、暗号管理サーバ１５０にアクセス要求する管理者の認証及びアクセス制御を実行する。さらに、アクセス制御プログラム２１０４は、暗号管理サーバ１５０にアクセス要求するストレージ装置１２０の認証及びアクセス制御を実行する。以上が暗号管理サーバ１５０のソフトウェア構成である。

【０３３２】

次に、本実施形態におけるストレージ装置１２０のソフトウェア構成を説明する。図２１に示す情報及びプログラムのうち、ＬＵ管理情報２０１、仮想ＬＵマッピング情報２０２、ストレージ装置機種・製造番号管理情報２０３、暗号鍵管理情報２０４、Ｉ／Ｏ処理プログラム２０５、暗号設定プログラム２０６及びストレージ管理プログラム２０９は、図２に示すものと同様である。このため、これらについての説明は省略する。

【０３３３】

ストレージ装置１２０の制御メモリ１２４には、上記の情報に加えて、暗号管理サーバ情報２１２１が格納される。

【０３３４】

図２４は、本発明の第３の実施形態の暗号管理サーバ情報２１２１の一例を示す説明図である。

【０３３５】

暗号管理サーバ情報２１２１は、項目２４０１で構成される。項目２４０１には、ストレージ装置１２０が送信する暗号鍵・暗号設定情報バックアップ情報２４１の送信先である暗号管理サーバ１５０のＩＰアドレス又はホスト名が格納される。ただし、項目２４０１には、ＩＰアドレス又はホスト名以外の、暗号管理サーバ１５０を一意に識別できる情報が格納されてもよい。

【０３３６】

図２０には、一つの暗号管理サーバ１５０のみを示すが、実際には、本実施形態の計算機システムは、複数の暗号管理サーバ１５０を備えてもよい。ストレージ装置１２０が暗号鍵・暗号設定情報バックアップ情報２４１を複数の暗号管理サーバ１５０に送信する場合、項目２４０１には、複数の暗号管理サーバ１５０の識別情報が格納される。

【０３３７】

次にストレージ装置１２０のプログラム情報について説明する。制御メモリ１２４には、上記のプログラムに加えて、暗号鍵・暗号設定情報バックアッププログラム２０７、暗号鍵・暗号設定情報リストアプログラム２０８及び暗号管理サーバ認証プログラム２１２２が格納される。

【０３３８】

本実施形態では、暗号鍵・暗号設定情報バックアッププログラム２０７は、暗号管理サーバ１５０に暗号鍵・暗号設定情報バックアップ情報２４１をバックアップする。暗号鍵・暗号設定情報リストアプログラム２０８は、暗号管理サーバ１５０から暗号鍵・暗号設定情報バックアップ情報２４１を受信してリストアを実行する。

【０３３９】

暗号管理サーバ認証プログラム２１２２は、ストレージ装置１２０が暗号管理サーバ１５０から暗号鍵・暗号設定情報バックアップ情報２４１を受信する時に、その暗号管理サーバ１５０を認証する。

【０３４０】

以上が本実施形態でのソフトウェア構成の説明である。次に本実施形態での暗号鍵・暗号設定情報のバックアップ・リストア処理について説明する。なお、図２２～図２４に示す情報、例えば管理者のアカウント情報や暗号管理サーバ１５０の情報及び送信元ストレージ装置等、は事前に登録済みであると仮定する。

【０３４１】

＜暗号管理サーバを用いたバックアップ処理＞

図２５は、本発明の第３の実施形態のストレージ装置１２０から暗号管理サーバ１５０へ暗号鍵・暗号設定情報をバックアップする処理の一例を示すフローチャートである。

【０３４２】

管理計算機１４０は、管理者からログイン要求を受信し（ステップ２５０１）、管理者を認証し（ステップ２５０２）、管理者認証に成功したか否かを判定する（ステップ２５０３）。

【０３４３】

認証に失敗した場合は処理を終了する。

【０３４４】

認証に成功した場合、管理者は、ストレージ装置１２０に暗号鍵・暗号設定情報のバックアップを指示する（ステップ２５０４）。

【０３４５】

指示を受けたストレージ装置１２０は、暗号鍵・暗号設定情報バックアップ情報２４１を暗号管理サーバ１５０へバックアップ（すなわち暗号鍵・暗号設定情報バックアップ情報２４１を暗号管理サーバ１５０へ送信）する（ステップ２５０５）。例えば、項目２４０１に格納された暗号管理サーバ１５０のアドレスへ暗号鍵・暗号設定情報バックアップ情報２４１が送信される。

【０３４６】

暗号鍵・暗号設定情報バックアップ情報２４１を受信した暗号管理サーバ１５０は、送信元のストレージ装置１２０を認証し（ステップ２５０６）、認証に成功したか否かを判定する（ステップ２５０７）。

【０３４７】

認証に失敗した場合は処理を終了する。

【０３４８】

認証に成功した場合、暗号管理サーバ１５０は、ストレージ装置１２０から受信した暗号鍵・暗号設定情報バックアップ情報２４１を統合管理する（ステップ２５０８）。

【０３４９】

＜暗号管理サーバを用いたリストア処理＞

図２６は、本発明の第３の実施形態の暗号管理サーバ１５０からストレージ装置１２０へ暗号鍵・暗号設定情報を送信し、リストアする処理の一例を示すフローチャートである。

【０３５０】

管理計算機１４０は、管理者からログイン要求を受信し（ステップ２６０１）、管理者を認証し（ステップ２６０２）、認証に成功したか否かを判定する（ステップ２６０３）。

【０３５１】

認証に失敗した場合は処理を終了する。

【０３５２】

認証に成功した場合、管理者は、管理計算機１４０から暗号管理サーバ１５０へログインを要求する（ステップ２６０４）。

【０３５３】
暗号管理サーバ１５０は、ログインを要求した管理者を認証し（ステップ２６０５）、認証に成功したか否かを判定する（ステップ２６０６）。
【０３５４】
認証に失敗した場合は処理を終了する。
【０３５５】
認証に成功した場合、管理者は、暗号管理サーバ１５０内の暗号鍵・暗号設定情報バックアップ情報２４１を指定し、それを管理者が指定するリストア先装置に送信するよう暗号管理サーバ１５０に指示する（ステップ２６０７）。例えば図２２の例では、管理者は項目２２０２の中からデータを指定し、リストア先装置を指定して、そのリストア先装置に項目２２０２のデータを送信するように暗号管理サーバ１５０に指示する。
【０３５６】
暗号管理サーバ１５０は、管理者から指定された暗号鍵・暗号設定情報のバックアップ情報を、指定されたリストア先装置に送信する（ステップ２６０８）。
【０３５７】
それを受信したリストア先装置は、送信元の暗号管理サーバ１５０を認証し（ステップ２６０９）、認証に成功したか否かを判定する（ステップ２６１０）。
【０３５８】
認証に失敗した場合は処理を終了する。
【０３５９】
認証に成功した場合、リストア先装置は、暗号管理サーバ１５０から送信された暗号鍵・暗号設定情報バックアップ情報２４１を受信し、受信した情報を使用して、図１３のステップ１３０２以降のリストア処理を実行する（ステップ２６１１）。
【０３６０】
以上が本実施形態での暗号鍵・暗号設定情報のバックアップ・リストア処理である。
【０３６１】
次に、本実施形態の第１の変形例について説明する。この変形例では、暗号鍵・暗号設定情報のリストアにあたり、管理者が暗号管理サーバ１５０へ暗号鍵・暗号設定情報の送信指示を出すのではなく、ストレージ装置１２０が暗号管理サーバ１５０へ直接暗号鍵・暗号設定情報の取得要求を送信する。以下では、上記で説明した処理とは異なる、暗号鍵・暗号設定情報のリストア処理についてのみ説明する。すなわち、この変形例における暗号鍵・暗号設定情報のバックアップ処理は、図２５に示したものと同じであるため、説明を省略する。
【０３６２】
＜暗号管理サーバを用いたリストア処理の変形例１＞
図２７は、本発明の第３の実施形態の暗号鍵・暗号設定情報バックアップ情報統合管理情報２１０１の第１の変形例を示す説明図である。
【０３６３】
図２７に示す暗号鍵・暗号設定情報バックアップ情報統合管理情報２１０１は、項目２２０１、２２０２及び２７０１の３つのデータ項目から構成される。
【０３６４】
項目２２０１及び２２０２は、図２２に示したものと同様であるため、説明を省略する。
【０３６５】
項目２７０１には、項目２２０２によって識別されるデータへのアクセスが許可されるストレージ装置１２０又は仮想先ストレージ装置１３０のＩＰアドレス又はホスト名が格納される。項目２７０１のデータはストレージ装置の機器認証に使用さる。このため、項目２７０１には、ストレージ装置を一意に識別できる情報である限り、ＩＰアドレス又はホスト名以外の情報が格納されてもよい。
【０３６６】

図２８は、本発明の第３の実施形態の管理者認証情報２１０２の第１の変形例を示す説明図である。

【０３６７】

管理者認証情報２１０２は、項目２３０１～２３０３の３つのデータ項目から構成される。これらの項目は、図２３に示したものと同様であるため、説明を省略する。

【０３６８】

ただし、この変形例では、ロール情報として、「管理サーバへアクセス可能なストレージ装置の登録」が格納される場合がある。例えば、ユーザＩＤ「ＡＢＣ」に対応するロール情報として「管理サーバへアクセス可能なストレージ装置の登録」が格納されている場合、ユーザＩＤ「ＡＢＣ」によって識別される管理者は、項目２２０２によって識別されるデータへのアクセスが許可されるストレージ装置を識別する情報を項目２７０１に新たに格納することができる。

【０３６９】

図２９は、本発明の第３の実施形態の暗号管理サーバ１５０からストレージ装置１２０へ暗号鍵・暗号設定情報を送信し、リストアする処理の第１の変形例を示すフローチャートである。

【０３７０】

管理計算機１４０は、管理者からログイン要求を受信し（ステップ２９０１）、管理者を認証し（ステップ２９０２）、認証に成功したか否かを判定する（ステップ２９０３）。

【０３７１】

認証に失敗した場合は処理を終了する。

【０３７２】

認証に成功した場合、管理者は、管理計算機１４０から暗号管理サーバ１５０へログインを要求する（ステップ２９０４）。

【０３７３】

暗号管理サーバ１５０は、ログインを要求した管理者を認証し（ステップ２９０５）、認証に成功したか否かを判定する（ステップ２９０６）。

【０３７４】

認証に失敗した場合は処理を終了する。

【０３７５】

認証に成功した場合、管理者は、暗号管理サーバ１５０内の暗号鍵・暗号設定情報バックアップ情報２４１を指定し、当該情報にアクセス可能なストレージ装置１２０として、新たにリストア先装置を追加する（ステップ２９０７）。

【０３７６】

例えば図２２の例では、先頭のエントリの項目２２０１に格納された「１０．１．１．１」によって識別されるストレージ装置１２０が故障して、その故障装置からバックアップされた情報をアドレス「Ａ１」によって識別されるリストア先装置にリストアしたい場合、管理者は、先頭エントリの項目２７０１に新たなリストア先装置のアドレス「Ａ１」を追加する。その結果、先頭エントリの項目２７０１には、「１０．１．１．１」及び「Ａ１」の二つのアドレスが格納される。

【０３７７】

次に、管理者は、管理計算機１４０からストレージ装置１２０に対し、管理者が指定したストレージ装置１２０の暗号鍵・暗号設定情報バックアップ情報２４１を、暗号管理サーバ１５０から取得し、リストアをするよう指示する（ステップ２９０８）。

【０３７８】

ストレージ装置１２０は、管理者に指定されたストレージ装置１２０の暗号鍵・暗号設定情報バックアップ情報２４１の取得を暗号管理サーバ１５０に要求する（ステップ２９０９）。

【０３７９】

暗号管理サーバ１５０は、暗号鍵・暗号設定情報バックアップ情報２４１の取得を要求したストレージ装置１２０（すなわちリストア先装置）を認証し（ステップ２９１０、ステップ２９１１）、認証に成功したか否かを判定する。

【０３８０】

認証に失敗した場合は処理を終了する。

【０３８１】

認証に成功した場合、暗号管理サーバ１５０は、リストア先装置に暗号鍵・暗号設定情報バックアップ情報２４１を送信する（ステップ２９１２）。ストレージ装置１２０は、暗号管理サーバ１５０から送られた暗号鍵・暗号設定情報バックアップ情報２４１を受信し、受信した情報を使用して、図１３のステップ１３０２以降のリストア処理を実行する（ステップ２９１３）。

【０３８２】

以上の本発明の実施形態によれば、例えば、計算機と、管理計算機と、仮想化機能及び暗号化機能を備える第１及び第２のストレージ装置（以下、仮想化制御ストレージ装置とも呼ぶ）と、仮想化制御ストレージ装置によって仮想化される一台以上の第３のストレージ装置（以下、仮想先ストレージ装置とも呼ぶ）で構成される計算機システムにおいて、第３のストレージ装置の記憶領域が第１のストレージ装置によって仮想化及び暗号化されている。第１のストレージ装置用の暗号鍵と、仮想先ストレージ装置用の暗号鍵を区別できるように、第１のストレージ装置の暗号鍵がバックアップされる。

【０３８３】

第１のストレージ装置が故障すると、第３のストレージ装置が第２のストレージ装置に新たに接続され、第２のストレージ装置に第１のストレージ装置からバックアップされた暗号鍵がリストアされる。この場合、第２のストレージ装置は以下の処理を行う。

【０３８４】

リストア要求された暗号鍵が、第２のストレージ装置からバックアップしたものか否かを判定する。その暗号鍵が第２のストレージ装置からバックアップされたものであり、かつ、第２のストレージ装置に暗号鍵が設定されていない場合、第２のストレージ装置は暗号鍵をリストアする。

【０３８５】

リストア要求された暗号鍵が第２のストレージ装置からバックアップされたものでない場合、第２のストレージ装置は、リストア要求された暗号鍵が、バックアップ元ストレージ装置（第１のストレージ装置）の自装置用の暗号鍵を含むか否かを判定する。含むと判定された場合、その第１のストレージ装置の自装置用の暗号鍵のリストアは実行されない。

【０３８６】

リストア要求された暗号鍵のうちその他の暗号鍵が、第２のストレージ装置自体が仮想化されていた場合の暗号鍵、又は、第２のストレージ装置が仮想化する第３のストレージ装置用の暗号鍵を含むか否かを判定する。含むと判定された場合は、その暗号鍵が第２のストレージ装置にリストアされる。

【０３８７】

以上の本発明の実施形態によれば、データの暗号・復号機能、暗号鍵・暗号設定情報のバックアップ・リストア機能及び仮想化機能を有するストレージ装置を含む計算機システムにおいて、ストレージ装置が故障しても、他のストレージ装置にその暗号鍵を誤ることなくリストアすることができる。このため、データ破壊を起こすことなく、暗号化された記憶領域のデータを復号することが可能である。

【０３８８】

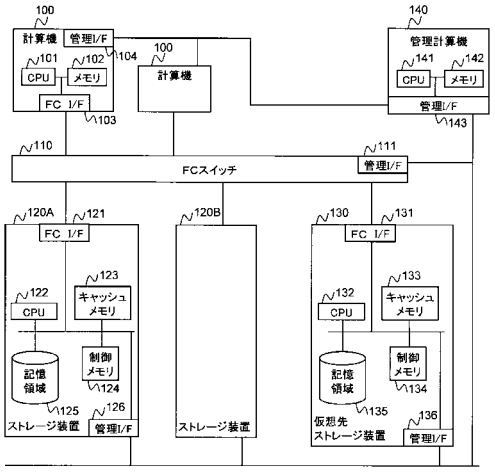
以上、実施の形態について説明したが、本発明はこうした実施の形態に何ら限定されるものではなく、本発明の趣旨を逸脱しない範囲内において様々な形態で実施し得ることは勿論である。

【図面の簡単な説明】

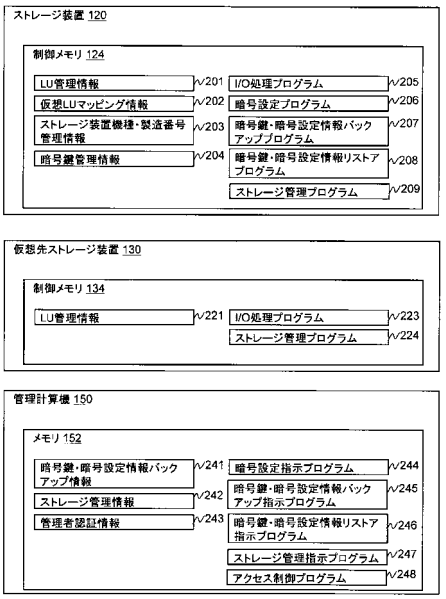
【０３８９】
【図１】本発明の第１の実施形態の計算機システムのハードウェア構成を示すブロック図である。
【図２】本発明の第１の実施形態の計算機システムのソフトウェア構成の一例を示す説明図である。
【図３】本発明の第１の実施形態のＬＵ管理情報の一例を示す説明図である。
【図４】本発明の第１の実施形態の仮想ＬＵマッピング情報の一例を示す説明図である。
【図５】本発明の第１の実施形態のストレージ装置機種・製造番号管理情報の一例を示す説明図である。
【図６】本発明の第１の実施形態の暗号鍵管理情報の一例を示す説明図である。
【図７】本発明の第１の実施形態の管理者認証情報の一例を示す説明図である。
【図８】本発明の第１の実施形態の暗号鍵・暗号設定情報バックアップ情報の一例を示す説明図である。
【図９】本発明の第１の実施形態のストレージ装置の暗号設定プログラムが実行する暗号設定処理の一例を示すフローチャートである。
【図１０】本発明の第１の実施形態の管理計算機の暗号鍵・暗号設定情報バックアップ指示プログラムが実行する暗号鍵・暗号設定情報のバックアップ処理の一例を示すフローチャートである。
【図１１】本発明の第１の実施形態のストレージ装置の暗号鍵・暗号設定情報バックアッププログラムが実行する暗号鍵・暗号設定情報のバックアップ処理の一例を示すフローチャートである。
【図１２】本発明の第１の実施形態の管理計算機の暗号鍵・暗号設定情報リストア指示プログラムがストレージ装置又は仮想先ストレージ装置に対して実行するリストア指示処理の一例を示すフローチャートである。
【図１３】本発明の第１の実施形態において管理計算機からリストア指示を受けたストレージ装置が実行するリストア処理の一例を示すフローチャートである。
【図１４】本発明の第１の実施形態において管理計算機からリストア指示を受けたストレージ装置が実行するリストア処理の第１の変形例を示すフローチャートである。
【図１５】本発明の第１の実施形態の管理計算機の暗号鍵・暗号設定情報リストア指示プログラムがストレージ装置又は仮想先ストレージ装置に対して実行するリストア指示処理の第１の変形例を示すフローチャートである。
【図１６】本発明の第１の実施形態の管理計算機の暗号鍵・暗号設定情報リストア指示プログラムがストレージ装置又は仮想先ストレージ装置に対して実行するリストア指示処理の第２の変形例を示すフローチャートである。
【図１７】本発明の第１の実施形態において管理計算機からリストア指示を受けたストレージ装置が実行するリストア処理の第２の変形例を示すフローチャートである。
【図１８】本発明の第２の実施形態の管理計算機のストレージ管理指示プログラムが実行するストレージ装置の監視処理の一例を示すフローチャートである。
【図１９】本発明の第２の実施形態の管理計算機の暗号鍵・暗号設定情報リストア指示プログラムが実行するストレージ装置へのリストア指示処理の一例を示すフローチャートである。
【図２０】本発明の第３の実施形態の計算機システムのハードウェア構成を示すブロック図である。
【図２１】本発明の第３の実施形態の計算機システムのソフトウェア構成の一例を示す説明図である。
【図２２】本発明の第３の実施形態の暗号鍵・暗号設定情報バックアップ情報統合管理情報の一例を示す説明図である。
【図２３】本発明の第３の実施形態の管理者認証情報の一例を示す説明図である。
【図２４】本発明の第３の実施形態の暗号管理サーバ情報の一例を示す説明図である。
【図２５】本発明の第３の実施形態のストレージ装置から暗号管理サーバへ暗号鍵・暗号

設定情報をバックアップする処理の一例を示すフローチャートである。
【図２６】本発明の第３の実施形態の暗号管理サーバからストレージ装置へ暗号鍵・暗号設定情報を送信し、リストアする処理の一例を示すフローチャートである。
【図２７】本発明の第３の実施形態の暗号鍵・暗号設定情報バックアップ情報統合管理情報の第１の変形例を示す説明図である。
【図２８】本発明の第３の実施形態の管理者認証情報の第１の変形例を示す説明図である。
【図２９】本発明の第３の実施形態の暗号管理サーバからストレージ装置へ暗号鍵・暗号設定情報を送信し、リストアする処理の第１の変形例を示すフローチャートである。
【符号の説明】
【０３９０】
１００　計算機
１０１、１２２、１３２、１４１　ＣＰＵ
１０２、１４２　メモリ
１０３、１２１、１３１　ファイバーチャネルインタフェース（ＦＣＩ／Ｆ）
１０４、１１１、１２６、１３６、１４３　管理Ｉ／Ｆ
１１０　ファイバーチャネル（ＦＣ）スイッチ
１２０Ａ、１２０Ｂ　ストレージ装置
１２３、１３３　キャッシュメモリ
１２４、１３４　制御メモリ
１２５、１３５　記憶領域（ＬＵ）
１３０　仮想先ストレージ装置

【図１】



【図２】



【図３】

LU管理情報201

301 ポート(WWN)	302 LU番号	303 容量	304 アクセス可能計算機(WWN)	305 仮想LU・実LU	306 暗号On/Off	307 鍵ID
CLA-1 (FF:00:00:00:00:00:00:FF)	1	100GB	10:00:00:00:00:00:00:70	実	Off	
	2	100GB	10:00:00:00:00:00:00:70	実	On	1
	3	100GB	20:00:00:00:00:00:A1:7A	仮想	On	2
…	…	…	…	…	…	…

【図４】

仮想LUマッピング情報202

401 ポート(WWN)	402 LU番号	403 仮想先装置機種・製造番号	404 ポート(WWN)	405 仮想先装置内LU番号
CLA-1 (FF:00:00:00:00:00:00:FF)	3	D600-100	A-1 (00:00:00:00:AA:AA:AA:AA)	1
	4	D600-100	A-1 (00:00:00:00:AA:AA:AA:AA)	2
	10	D700-110	AA-1(00:00:00:00:BB:BB:BB:BB)	1
…	…	…	…	…

【図５】

ストレージ装置機種・製造番号管理情報203

501 自ストレージ装置機種・製造番号	502 アドレス	503 モード	504 仮想先装置機種・製造番号
A500-10011	10.1.1.1	通常	D600-100
			D700-110
			⋮

【図６】

暗号鍵管理情報204

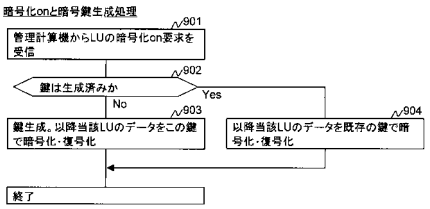
601 鍵ID	602 鍵のデータ	603 鍵長	604 アルゴリズム	605 鍵適用装置	606 仮想先装置機種・製造番号	607 鍵適用LU
1	O35tuobdg5j6ki…	256	AES-ECB	自		LU2
2	l0cc-ai0-ci0ags…	256	AES-ECB	仮想先	D600-100	LU1
3	052pgrmkg3jp9…	128	AES-ECB	仮想先	D600-100	LU2
4	0jfwi0fwj9ew09…	128	AES-ECB	仮想先	D600-100	LU3
5	65p54m13lp5kl…	128	AES-CBC	仮想先	D700-110	装置
…	…	…	…	…	…	…

【図７】

管理者認証情報243

701 ユーザID	702 パスワード	703 ロール
aaa	Abiec…	セキュリティ管理者
bbb	39ivjpa…	ストレージ管理者
10001	dpfapo…	アカウント管理者
…	…	…

【図９】



【図８】

暗号鍵・暗号設定情報バックアップ情報241

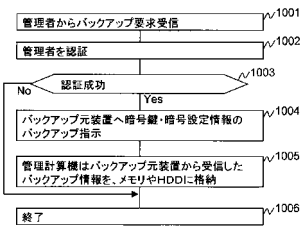
図3、図4の複製情報 801

＋

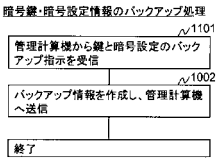
図6鍵管理情報のバックアップ 情報 810

811 バックアップ元装置機種・製造番号	812 鍵ID	813 鍵のデータ	814 鍵長	815 アルゴリズム	816 鍵適用装置	817 仮想先装置機種・製造番号	818 鍵適用LU
A500-10011	1	O35tuobdg5j6ki…	256	AES-ECB	自		LU2
	2	l0cc-ai0-ci0ags…	256	AES-ECB	仮想先	D600-100	LU1
	3	052pgrmkg3jp9…	128	AES-ECB	仮想先	D600-100	LU2
	4	0jfwi0fwj9ew09…	128	AES-ECB	仮想先	D600-100	LU3
	5	65p54m13lp5kl…	128	AES-CBC	仮想先	D700-110	装置
	…	…	…	…	…	…	…

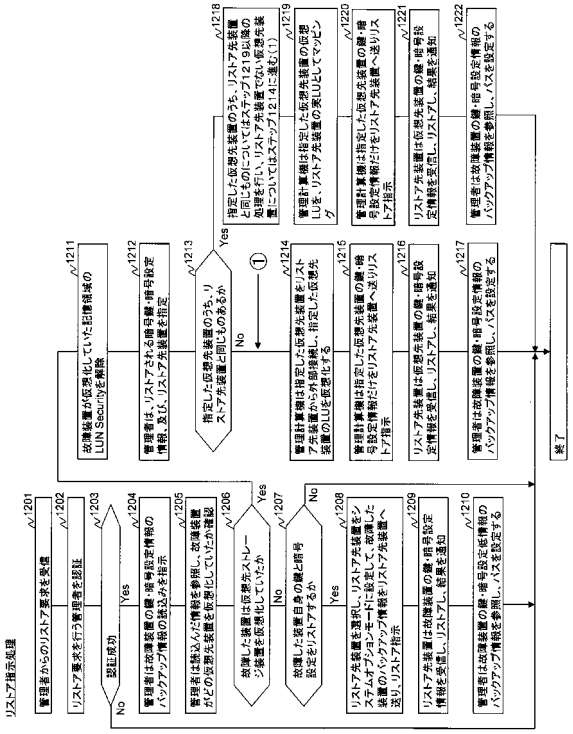
【図１０】



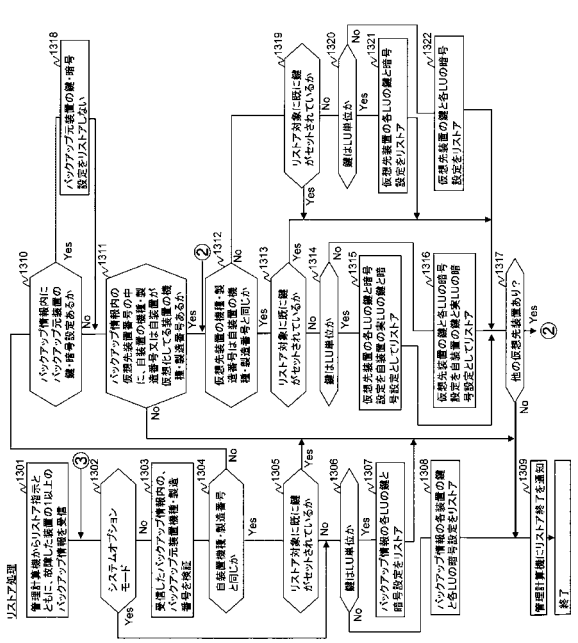
【図１１】



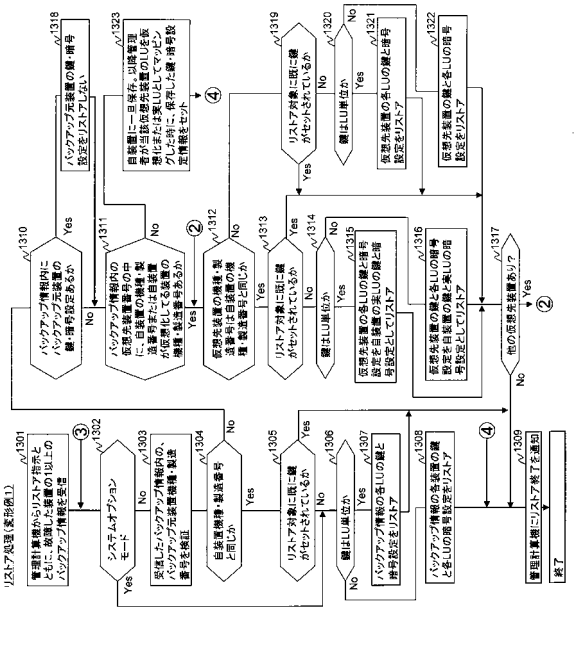
【図１２】



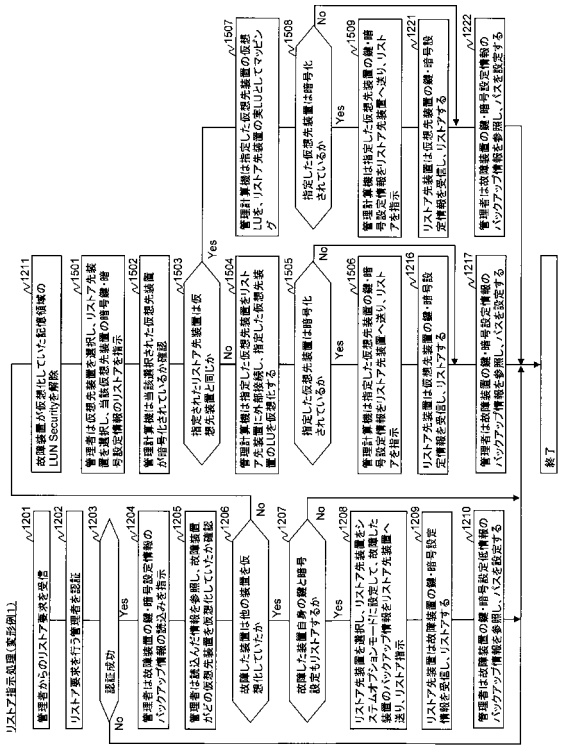
【図１３】



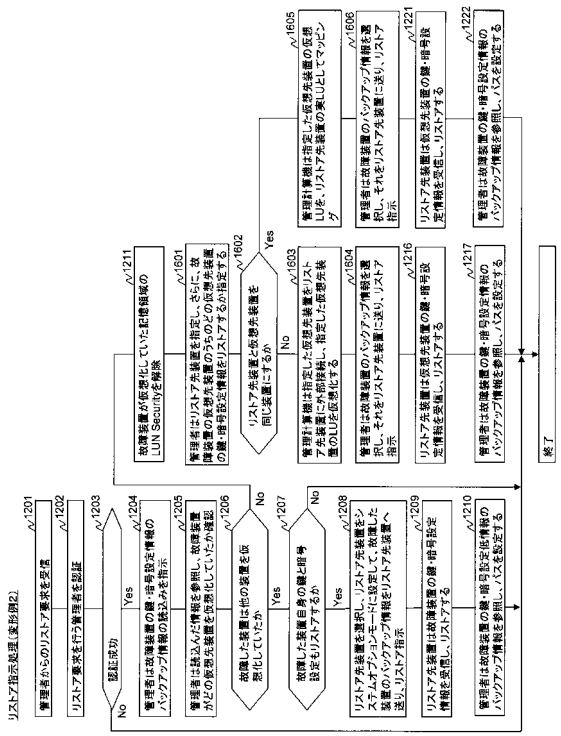
【図１４】



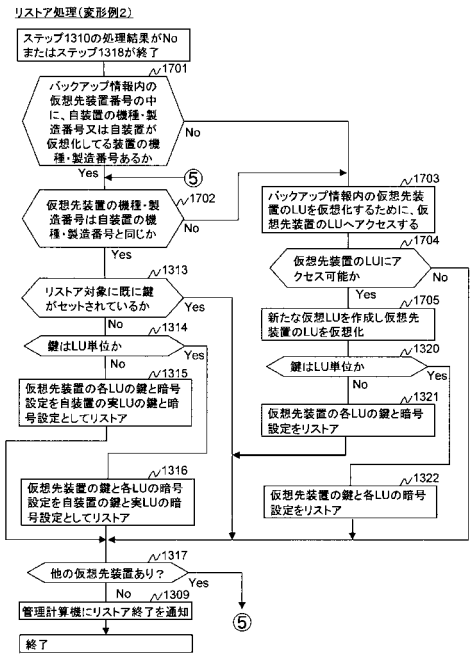
【図１５】



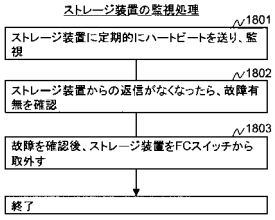
【図１６】



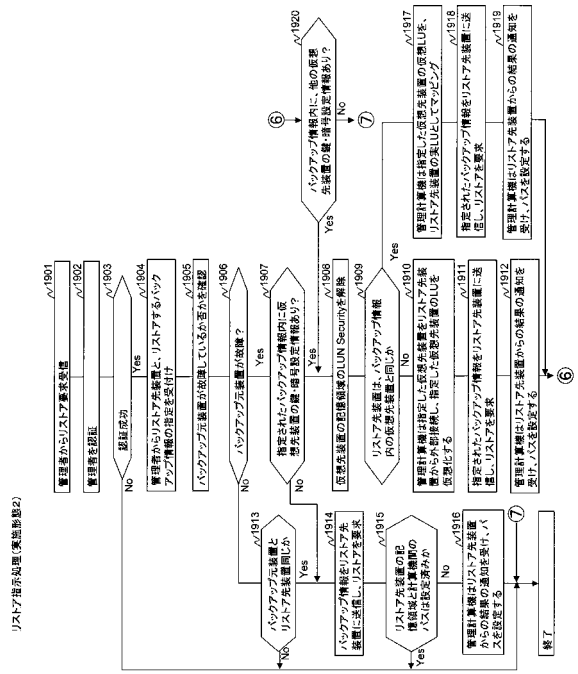
【図１７】



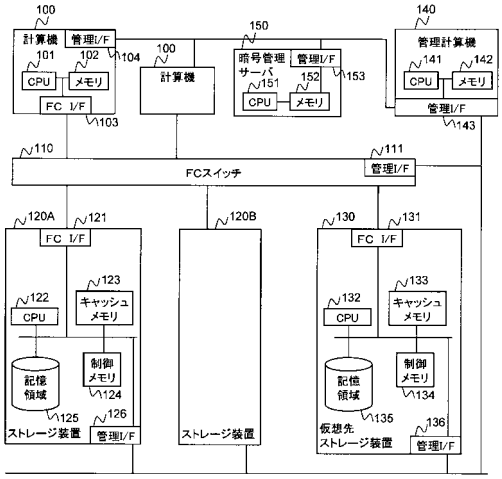
【図１８】



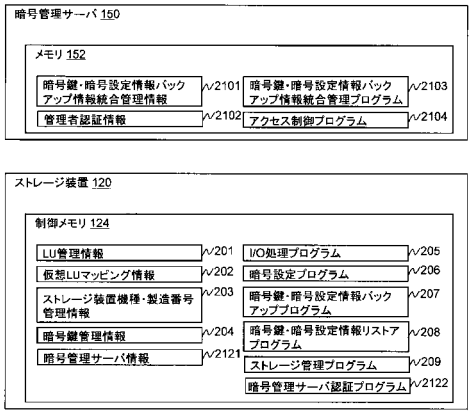
【図１９】



【図２０】



【図２１】



【図２２】

暗号鍵・暗号設定情報バックアップ情報統合管理情報2101

2201 暗号鍵・暗号設定情報送信元ストレージ装置	2202 暗号鍵・暗号設定情報バックアップ情報	2203 アクセス可能な管理者
10.1.1.1	A500-1 key_bkup	ABC
Controller 2	A500-2 key_bkup	ABC
10.1.1.10	A600-10 key_bkup	DDD
Controller D1	D500-1 key_bkup	aiu7, DDD
…	…	…

【図２３】

管理者認証情報2102

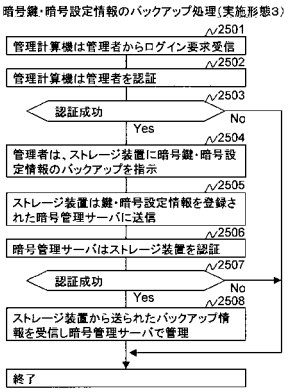
2301 ユーザID	2302 パスワード	2303 ロール
ABC	Abiec…	暗号鍵・暗号設定情報バックアップ情報の送信指示
DDD	dpfapo…	管理サーバのアカウント管理
…	…	…

【図２４】

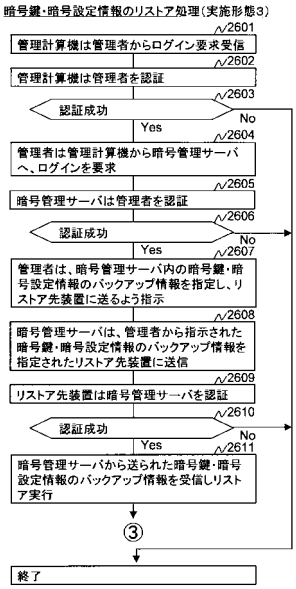
暗号管理サーバ情報2121

2401 暗号管理サーバ
190.1.1.1
190.10.1.1
…

【図２５】



【図２６】



【図２７】

暗号鍵・暗号設定情報バックアップ情報統合管理情報2101

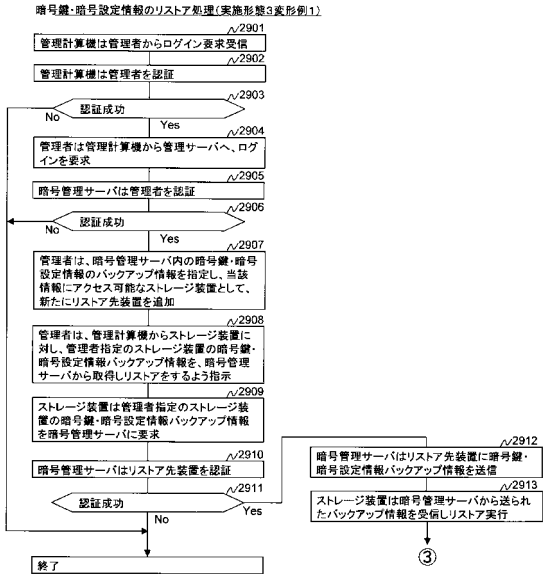
2201 暗号鍵・暗号設定情報送信元ストレージ装置	2202 暗号鍵・暗号設定情報バックアップ情報	2701 アクセス可能なストレージ装置
10.1.1.1	A500-1 key_bkup	10.1.1. 1
Controller 2	A500-2 key_bkup	Controller 2 10.1.1.1
10.1.1.10	A600-10 key_bkup	10.1.1.10
Controller D1	D500-1 key_bkup	Controller D1
…	…	…

【図２８】

管理者認証情報2102

2301 ユーザID	2302 パスワード	2303 ロール
ABC	Abiec…	管理サーバへアクセス可能なストレージ装置の登録
DDD	dpfapo…	管理サーバのアカウント管理
…	…	…

【図２９】



フロントページの続き

(72)発明者　藤井　健司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　大崎　伸之
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　和田　財太

(56)参考文献　特開２００７－０２８５０２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　３／０６