(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2006-114029
(P2006-114029A)
(43)公開日　平成18年4月27日(2006.4.27)

| (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 12/14 | 520B | 5B065 |
| | | G06F 12/14 | 540A | |

審査請求 未請求　請求項の数 51　ＯＬ　外国語出願　（全 19 頁）

(21)出願番号　特願2005-281078 (P2005-281078)
(22)出願日　平成17年9月28日 (2005.9.28)
(31)優先権主張番号　10/965064
(32)優先日　平成16年10月15日 (2004.10.15)
(33)優先権主張国　米国 (US)

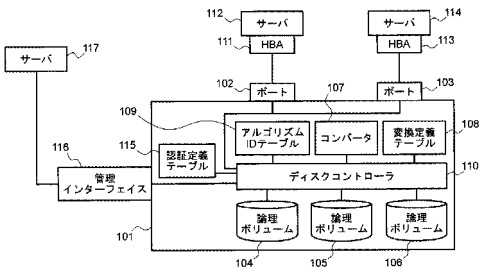
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075096
弁理士　作田　康夫
(74)代理人　100100310
弁理士　井上　学
(72)発明者　大崎　伸之
アメリカ合衆国カリフォルニア州キャンベル　エラムアベニュー　１２８１

Ｆターム(参考)　5B017 AA03 BA06 BA07 CA07
5B065 BA01 BA07 PA02 PA04 PA11 PA16

(54)【発明の名称】データストレージに対する方法と装置

(57)【要約】
【課題】
不必要な安全ギャップを避けるために、ストレージシステムを出る全てのデータは安全を守る必要がある。
【解決手段】
ストレージシステムの重要なデータの予期しない露出を避けるための装置、システム、および方法はデータ転送に関する許可と変換の情報を有するテーブルを含む。ストレージシステムが一つの論理装置またはボリュームから他の領域、例えばホスト、テープストレージまたはストレージシステムの内部または外部の他の論理装置またはボリュームへ一定のセットのデータを転送する時に、ストレージシステムはテーブルを参照して転送が許可されているかおよびデータの変換が転送の前に要求されているかを決定する。ストレージコントローラはもしも必要ならばデータを変換して、もしも許可されているならばターゲットの行先にデータを転送する。データを安全化する管理が集中化されるようにキーはストレージシステム内に保持される。
【選択図】　図１

図１



【特許請求の範囲】
【請求項１】
複数の論理装置と、
前記の複数の論理装置から選択された一つの装置と前記の複数の論理装置から選択された他の装置またはディスクコントローラが接続されている他の装置の間のデータ転送を制御し、前記の複数の論理装置にアクセスするディスクコントローと、
前記の一つの装置と前記の他の装置の間の前記のデータ転送に関するルールを有する変換定義テーブルと
を備え、
前記の変換定義テーブルが前記の一つの装置に保存されたデータの状態を含む情報および前記の他の装置が前記の一つの装置に保存された前記のデータへのアクセス許可を有するかについての情報を有することを特徴とするストレージシステム。
【請求項２】
前記の他の装置が前記の一つの装置に保存された前記のデータに対してアクセス許可を有する時に、前記の変換定義テーブルが前記の一つの装置からのデータが転送の間に復号化されるかまたは解凍される必要があるか、および前記のデータが前記の他の装置への転送の間に続けて暗号化されるかまたは圧縮される必要があるかを定義することを特徴とする、請求項１に記載のストレージシステム。
【請求項３】
前記の他の装置が暗号化されたデータを要求するケースでは、前記の一つの装置からのデータが転送の間に暗号化されることを特徴とする、請求項２に記載のストレージシステム。
【請求項４】
前記の他の装置が圧縮されたデータを要求するケースでは、前記の一つの装置からのデータが転送の間に圧縮されることを特徴とする、請求項２に記載のストレージシステム。
【請求項５】
前記の他の装置が暗号化および圧縮を要求するケースでは、データが最初に暗号化されて次に圧縮されることを特徴とする、請求項２に記載のストレージシステム。
【請求項６】
暗号化に対する適切な属性がアルゴリズムＩＤテーブルから選択されることを特徴とする、請求項３に記載のストレージシステム。
【請求項７】
圧縮に対する適切な属性がアルゴリズムＩＤテーブルから選択されることを特徴とする、請求項４に記載のストレージシステム。
【請求項８】
暗号化および圧縮に対する適切な属性がアルゴリズムＩＤテーブルから選択されることを特徴とする、請求項５に記載のストレージシステム。
【請求項９】
前記の一つの装置が暗号化されたデータを有するケースでは、前記の暗号化されたデータが転送の間に復号化されることを特徴とする、請求項２に記載のストレージシステム。
【請求項１０】
前記の一つの装置が圧縮されたデータを有するケースでは、前記の圧縮されたデータが転送の間に解凍されることを特徴とする、請求項２に記載のストレージシステム。
【請求項１１】
前記の一つの装置が暗号化および圧縮されたデータを有するケースでは、前記のデータが転送の間に解凍され次に復号化されることを特徴とする、請求項２に記載のストレージシステム。
【請求項１２】

前記の一つの装置と前記の他の装置が同じ状態を有するケースでは、前記のデータが直接転送されることを特徴とする、請求項２に記載のストレージシステム。
【請求項１３】
前記の他の装置がテープドライブであることを特徴とする、請求項１に記載のストレージシステム。
【請求項１４】
前記の他の装置が遠隔ストレージシステムであることを特徴とする、請求項１に記載のストレージシステム。
【請求項１５】
前記の変換定義テーブルが管理目的で遠隔的にアクセスされることができることを特徴とする、請求項１に記載のストレージシステム。
【請求項１６】
前記の変換定義テーブルの前記の論理装置の少なくとも一つに対するデフォルト設定が、他のどれかの装置に転送する前にいつも暗号化するように設定されることを特徴とする、請求項１に記載のストレージシステム。
【請求項１７】
前記の一つの装置に保存されたデータの状態が第一のアルゴリズムＩＤで暗号化される時に、前記のデータは、前記のデータの前記の暗号化が前記の第一のアルゴリズムＩＤから前記の第一のアルゴリズムＩＤと異なる第二のアルゴリズムＩＤに変換される再キー設定処理を受けることを特徴とする、請求項１に記載のストレージシステム。
【請求項１８】
前記の一つの装置に保存された前記のデータの全部の前記の暗号化が前記の第一のアルゴリズムＩＤから前記の第二のアルゴリズムＩＤに変換されるまで、前記のディスクコントローラが、ブロックごとをベースとして前記のデータを読み出すことおよび前記の第一と第二のアルゴリズムＩＤを使用して前記のデータを変換することによって、前記の再キー設定処理を実行することを特徴とする、請求項１７に記載のストレージシステム。
【請求項１９】
データを保存し、およびストレージシステムの内部の場所から前記のストレージシステムの内部または外部のターゲットにデータを転送するための方法において、
前記の場所から前記のターゲットにデータを転送する要求を受け取るステップと、
前記のターゲットを含む複数のターゲットへのデータの転送に対する許可と変換要求を記述する第一のテーブルを提供するステップと、
前記の場所から前記のターゲットへの前記のデータの転送が許可されるかを決定するために前記の第一のテーブルを調べるステップと、
もしも前記のターゲットへの前記のデータの転送が許可されるなら、前記のデータの変換が要求されるかを決定するために前記の第一のテーブルを調べ、もしも変換が要求されるなら、前記のデータを変換されたデータに変換するステップと、
もしも転送が許可されておよび変換が要求されないなら、前記のターゲットに前記のデータを転送し、またはもしも転送が許可されておよび変換も要求されるなら、前記の変換されたデータを前記のターゲットに転送するステップと
から成ることを特徴とする方法。
【請求項２０】
前記の場所の状態と前記のターゲットの状態を示す通知を前記の第一のテーブルに提供するステップをさらに含み、データの変換が要求されるか決定するために前記の第一のテーブルを調べる前記のステップが、前記の場所の状態を前記のターゲットの状態と比較するステップを含むことを特徴とする、請求項１９に記載の方法。
【請求項２１】
もしも前記のターゲットの状態が前記の場所の状態に一致するなら、変換は要求されないので、前記のデータの変換が要求されるか決定するために前記の第一のテーブルを調べる前記のステップが、前記の場所の状態を前記のターゲットの状態と比較するステップ

を含むことを特徴とする、請求項２０に記載の方法。
【請求項２２】
もしも前記のターゲットの状態が前記の場所の状態に一致しないなら、前記のデータを変換するステップをさらに含むことを特徴とする、請求項２１に記載の方法。
【請求項２３】
前記の場所の状態と前記のターゲットの状態を示す通知を前記の第一のテーブルに提供する前記のステップが、前記のデータの圧縮または解凍が前記のデータの転送の前に要求されるかを示す通知を提供するステップを含むことを特徴とする、請求項２０に記載の方法。
【請求項２４】
前記の場所の状態と前記のターゲットの状態を示す通知を前記の第一のテーブルに提供する前記のステップが、前記のデータの暗号化または復号化が前記のデータの転送の前に要求されるかを示す通知を提供するステップを含むことを特徴とする、請求項２０に記載の方法。
【請求項２５】
もしも前記のデータの暗号化または復号化が要求されるなら、アルゴリズムＩＤを提供するステップをさらに含むことを特徴とする、請求項２４に記載の方法。
【請求項２６】
各前記のアルゴリズムＩＤに関連する暗号化／復号化アルゴリズムのキーを示す第二のテーブルを提供するステップをさらに含み、前記のデータを変換する前記のステップが前記のデータの暗号化または復号化に対する前記のアルゴリズムＩＤを使用するステップを含むことを特徴とする、請求項２５に記載の方法。
【請求項２７】
もしも圧縮または解凍が要求されるなら、アルゴリズムＩＤを提供するステップをさらに含むことを特徴とする、請求項２３に記載の方法。
【請求項２８】
各前記のアルゴリズムＩＤに関連する圧縮／解凍アルゴリズムのキーを示す第二のテーブルを提供するステップをさらに含み、前記のデータを変換する前記のステップが前記のデータの圧縮または解凍に対する前記のアルゴリズムＩＤを使用するステップを含むことを特徴とする、請求項２７に記載の方法。
【請求項２９】
前記のデータを保存しおよび前記の場所と前記のターゲットの間の前記のデータを転送することを制御するためにディスクコントローラを提供するステップをさらに含むことを特徴とする、請求項１９に記載の方法。
【請求項３０】
データを保存し転送するためのシステムにおいて、
サーバと、
複数の論理装置と、
前記のサーバと前記の複数の論理装置の間に接続されるディスクコントローラと、
データが前記のサーバと前記の複数の論理装置のどれかとの間で転送されることが可能であるかおよびその方法に関して、およびデータが一つの論理装置と他の論理装置の間で転送されることが可能であるかおよびその方法に関してのルールを有する変換定義テーブルと
を備えるストレージシステムと
を備え、
前記の変換定義テーブルが、前記の複数の論理装置または前記のサーバから選択された一つの装置に保存されたデータの状態、および前記の複数の論理装置、前記のサーバ、または他のいずれかの装置から選択された他の装置がそのようなデータに対するアクセス許可を有するかを含む情報を有する

ことを特徴とするシステム。
【請求項３１】
前記の他の装置が前記の一つの装置に保存された前記のデータに対するアクセス許可を有する時に、前記の変換定義テーブルは、前記の一つの装置からのデータが転送の間に復号化されるかまたは解凍される必要があるか、および前記のデータが前記の他の装置、サーバまたは他の装置への転送の間に暗号化されるかまたは圧縮される必要があるかを定義することを特徴とする、請求項３０に記載のシステム。
【請求項３２】
前記の他の装置、サーバまたは他の装置が暗号化されたデータを要求するケースでは、前記の一つの装置からのデータが転送の間に暗号化されることを特徴とする、請求項３１に記載のシステム。
【請求項３３】
前記の他の装置、サーバまたは他の装置が圧縮されたデータを要求するケースでは、前記の一つの装置からのデータが転送の間に圧縮されることを特徴とする、請求項３１に記載のシステム。
【請求項３４】
前記の他の装置、サーバまたは他の装置が暗号化と圧縮を要求するケースでは、前記のデータが最初に暗号化され次に圧縮されることを特徴とする、請求項３１に記載のシステム。
【請求項３５】
暗号化に対する適切な属性がアルゴリズムＩＤテーブルから選択されることを特徴とする、請求項３２に記載のシステム。
【請求項３６】
圧縮に対する適切な属性がアルゴリズムＩＤテーブルから選択されることを特徴とする、請求項３３に記載のシステム。
【請求項３７】
暗号化と圧縮に対する適切な属性がアルゴリズムＩＤテーブルから選択されることを特徴とする、請求項３４に記載のシステム。
【請求項３８】
前記の一つの装置が暗号化されたデータを有するケースでは、前記の暗号化されたデータが転送の間に復号化されることを特徴とする、請求項３１に記載のシステム。
【請求項３９】
前記の一つの装置が圧縮されたデータを有するケースでは、前記の圧縮されたデータが転送の間に解凍されることを特徴とする、請求項３１に記載のシステム。
【請求項４０】
前記の一つの装置が暗号化および圧縮されたデータを有するケースでは、前記のデータが転送の間に解凍され次に復号化されることを特徴とする、請求項３１に記載のシステム。
【請求項４１】
前記の一つの装置に保存されたデータの前記の状態が第一のアルゴリズムＩＤで暗号化される時に、前記のデータは、前記のデータの前記の暗号化が前記の第一のアルゴリズムＩＤから前記の第一のアルゴリズムＩＤと異なる第二のアルゴリズムＩＤに変換される再キー設定処理を受けることを特徴とする、請求項３０に記載のストレージシステム。
【請求項４２】
前記の一つの装置に保存された前記のデータの全部の前記の暗号化が前記の第一のアルゴリズムＩＤから前記の第二のアルゴリズムＩＤに変換されるまで、前記のディスクコントローラが、ブロックごとをベースとして前記のデータを読み出すことおよび前記の第一と第二のアルゴリズムＩＤを使用して前記のデータを変換することによって、前記の再キー設定処理を実行することを特徴とする、請求項４１に記載のストレージシステム。
【請求項４３】

前記の一つの装置と前記の他の装置が同じ状態を有するケースでは、前記のデータが直接転送されることを特徴とする、請求項３１に記載のシステム。
【請求項４４】
前記の他の装置がテープドライブであることを特徴とする、請求項３０に記載のシステム。
【請求項４５】
前記の他の装置が遠隔ストレージシステムであることを特徴とする、請求項３０に記載のシステム。
【請求項４６】
前記の変換定義テーブルが管理目的で遠隔的にアクセスされることが可能であることを特徴とする、請求項３０に記載のシステム。
【請求項４７】
前記の変換定義テーブルの前記の論理装置の少なくとも一つに対するデフォルト設定が、他のどれかの論理装置、サーバまたは他の装置に転送する前にいつも暗号化するように設定されることを特徴とする、請求項３０に記載のシステム。
【請求項４８】
一つの装置と他の装置の間でデータを転送する方法において、
前記の一つの装置と前記の他の装置の間の情報の転送に関する情報を変換定義テーブルに保存するステップと、
前記の他の装置からの転送要求および前記の一つの装置からのデータの転送の通知を受け取るステップと、
前記の変換定義テーブルから転送に関する前記の情報を検索するステップと、
もしも前記の情報が転送は許可されないことを示しているなら、いかなるデータも転送しないステップと、
もしも前記の情報が転送は許可されることを示しているなら、要求された転送の特定の方向が許可されているかおよび暗号化／復号化または圧縮／解凍が要求されているかを含む、それによって情報が転送されるパラメータを決定するステップと、
から成ることを特徴とする方法。
【請求項４９】
前記の変換定義テーブルが前記の一つの装置と前記の他の装置に加えて他の複数の装置に関する転送情報を保存することを特徴とする、請求項４８に記載の方法。
【請求項５０】
前記の他の装置が前記のストレージシステムの外部にあり前記のストレージシステムに接続されている装置であることを特徴とする、請求項１に記載のストレージシステム。
【請求項５１】
前記の他の複数の装置が前記のストレージシステムの外部であり前記のストレージシステムに接続されている装置を含むことを特徴とする、請求項４９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】
０００１　本発明はデータストレージに、より具体的には、データが許可されていないアクセスから保護される安全なデータストレージに対するアクセス制御技術に関係する。
【背景技術】
【０００２】
０００２　データは許可されていないアクセスから保護される必要がある貴重な法人の財産であることが知られている。アクセス制御技術は許可されていないユーザが許可なくデータにアクセスすることを防止する。既知の技術はＷＯ００５５７５０Ａ１および米国特許ＮＯ６，６８４，２０９Ｂ１にそれぞれ開示されているようなゾーニングまたはＬ

Uマスキングを含み、特定のホストに対して一定のデータボリュームまたはストレージシステムへのアクセスを制限する。コンピュータシステムに対するオペレーティングシステムはまたユーザ特権管理機能を備えている。

【０００３】

０００３　しかし、従来の技術システムはこのようなアクセス制御によって保護できない安全ギャップを置き忘れている。例えば、ストレージシステムがアクセス制御メカニズムによって保護される時でさえも、テープまたは遠隔ストレージシステムにコピーされたデータが破壊され易い場合があり、またはテープまたは磁気ディスクが物理的に盗まれる場合がある。

【０００４】

０００４　このような出来事が起こる理由の一つはアクセス制御がクライアント、サーバ、スイッチ、およびストレージシステムなどの多くの構成要素によって実施されることである。ストレージシステムが、認証されているサーバにだけアクセスを許可する時にさえ、もしもサーバの一つでもユーザ特権を安全に管理しないと安全は有効でなくなり得る。例えば、スイッチのような装置は、これはホストとストレージシステムの間に存在しているが、ストレージシステムから出て来るデータを変換することができる。しかし、もしも全てのスイッチを監視することを試みると、多量なデータと同じく多数の装置を管理することになり、これはストレージエリアネットワーク（ＳＡＮ）の組織管理を非常に複雑にするであろう。これはまた多数の装置に対して安全を確保する必要のある管理者に懸かる責任を増やすことになる。さらに、このような方法では、デフォルト設定を使用してデータの予期しない露出を避けるためにストレージシステムにおける全ての保存データを暗号化する必要があり、これは、もしもキーとアルゴリズム情報が失われるとオリジナルデータが失われるリスクを増やすことになる。

【０００５】

０００５　安全破壊のもう一つの理由は、秘密のデータを有するボリュームをアクセスできる人達がデータの内容を必ずしも理解する必要がない場合がしばしば起きることである。例えば、ストレージシステムからテープへのデータの遠隔コピーを行うストレージ管理者がビジネスアプリケーションによって生成されたデータの意味を理解する必要がない場合がある。このような不必要な安全ギャップを避けるために、ストレージシステムを出る全てのデータは別に認められていない限り安全を守る必要がある。

【０００６】

０００６　ＷＯ２００２０９３３１４Ａ２は、装置がホストとストレージシステムの間に存在しそれらの間のコミュニケーションをチェックするネットワークストレージに対する暗号化ベースの安全システムを開示する。装置はストレージシステム方向へのデータを暗号化して、ホスト方向へのデータを復号化する。従ってストレージシステム内の全てのデータは暗号化される。

【０００７】

０００７　米国特許ＮＯ．５，２３５，６４１はファイル暗号化方法とストレージシステムのデータを暗号化および復号化するファイル暗号システムを開示しており、キー生成機能をホスト側に置いている。

【０００８】

０００８　米国特許ＮＯ．５，９４０，５０７はシステムで保存されるデータを暗号化することによってアーカイブ／バックアップサポートにプライバシ保証を提供する情報処理システムを開示している。

【０００９】

０００９　ＤＥＳ（ｄａｔａ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ）に関する情報はＤＡＴＡ ＥＮＣＲＹＰＴＩＯＮ ＳＴＡＮＤＡＲＤ（ＤＥＳ）、Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ Ｐｕｂｌｉｃａｔｉｏｎｓ（ＦＩＰＳ Ｐｕｂ ４６－２）、Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕ ｏｆ Ｓｔａｎｄａｒｄｓ，１９８８、ｈｔｔｐ：／／ｗｗｗ．ｉｔｌ．ｎｉｓｔ．ｇｏｖ／

ｆｉｐｓｐｕｂｓ／ｆｉｐ４６－２．ｈｔｍにおいて見つけることができる。
【００１０】
００１０　ＡＥＳ（ａｄｖａｎｃｅｄ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ）に関する情報はＡＤＶＡＮＣＥＤ ＥＮＣＲＹＰＴＩＯＮ ＳＴＡＮＤＡＲＤ（ＡＥＳ）、Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ Ｐｕｂｌｉｃａｔｉｏｎｓ（ＦＩＰＳ Ｐｕｂ １９７）、Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕ ｏｆ Ｓｔａｎｄａｒｄｓ，２００１、ｈｔｔｐ：／／ｃｓｒｃ．ｎｉｓｔ．ｇｏｖ／ＣｒｙｐｔｏＴｏｏｌｋｉｔ／ａｅｓ／において見つけることができる。
【００１１】
００１１　ＷＯ００５５７５０Ａ１；ＷＯ２００２０９３３１４Ａ２；米国特許Ｎｏ．５，２３５，６４１；米国特許Ｎｏ．５，９４０，５０７；および米国特許Ｎｏ．６，６８４，２０９Ｂ１の完全な開示内容はここに参考として提供される。
【００１２】
【特許文献１】国際公開第００／５５７５０号
【特許文献２】米国特許第６，６８４，２０９号
【特許文献３】国際公開第０２／０９３３１４号
【特許文献４】米国特許第５，２３５，６４１号
【特許文献５】米国特許第５，９４０，５０７号
【非特許文献１】ＥＮＣＲＹＰＴＩＯＮ ＳＴＡＮＤＡＲＤ（ＤＥＳ）、[online]、Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ Ｐｕｂｌｉｃａｔｉｏｎｓ（ＦＩＰＳ Ｐｕｂ ４６－２）、Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕ ｏｆ Ｓｔａｎｄａｒｄｓ，１９８８、ｈｔｔｐ：／／ｗｗｗ．ｉｔｌ．ｎｉｓｔ．ｇｏｖ／ｆｉｐｓｐｕｂｓ／ｆｉｐ４６－２．ｈｔｍ
【非特許文献２】ＡＤＶＡＮＣＥＤ ＥＮＣＲＹＰＴＩＯＮ ＳＴＡＮＤＡＲＤ（ＡＥＳ）、[online]、Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ Ｐｕｂｌｉｃａｔｉｏｎｓ（ＦＩＰＳ Ｐｕｂ １９７）、Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕ ｏｆ Ｓｔａｎｄａｒｄｓ，２００１、ｈｔｔｐ：／／ｃｓｒｃ．ｎｉｓｔ．ｇｏｖ／ＣｒｙｐｔｏＴｏｏｌｋｉｔ／ａｅｓ／
【発明の開示】
【発明が解決しようとする課題】
【００１３】
０００３　しかし、従来の技術システムはこのようなアクセス制御によって保護できない安全ギャップを置き忘れている。例えば、ストレージシステムがアクセス制御メカニズムによって保護される時でさえも、テープまたは遠隔ストレージシステムにコピーされたデータが破壊され易い場合があり、またはテープまたは磁気ディスクが物理的に盗まれる場合がある。
【００１４】
０００４　このような出来事が起こる理由の一つはアクセス制御がクライアント、サーバ、スイッチ、およびストレージシステムなどの多くの構成要素によって実施されることである。ストレージシステムが、認証されているサーバにだけアクセスを許可する時にさえ、もしもサーバの一つでもユーザ特権を安全に管理しないと安全は有効でなくなり得る。例えば、スイッチのような装置は、これはホストとストレージシステムの間に存在しているが、ストレージシステムから出て来るデータを変換することができる。しかし、もしも全てのスイッチを監視することを試みると、多量なデータと同じく多数の装置を管理することになり、これはストレージエリアネットワーク（ＳＡＮ）の組織管理を非常に複雑にするであろう。これはまた多数の装置に対して安全を確保する必要のある管理者に懸かる責任を増やすことになる。さらに、このような方法では、デフォルト設定を使用してデータの予期しない露出を避けるためにストレージシステムにおける全ての保存データを暗号化する必要があり、これは、もしもキーとアルゴリズム情報が失われるとオリジナルデータが失われるリスクを増やすことになる。

【００１５】
０００５　安全破壊のもう一つの理由は、秘密のデータを有するボリュームをアクセスできる人達がデータの内容を必ずしも理解する必要がない場合がしばしば起きることである。例えば、ストレージシステムからテープへのデータの遠隔コピーを行うストレージ管理者がビジネスアプリケーションによって生成されたデータの意味を理解する必要がない場合がある。このような不必要な安全ギャップを避けるために、ストレージシステムを出る全てのデータは別に認められていない限り安全を守る必要がある。
【課題を解決するための手段】
【００１６】
００１２　本発明はデータストレージに対する方法、装置、およびシステムに向けられている。ストレージシステムが一つのボリュームから他のエリア、例えばホスト、テープストレージ、またはストレージシステム内部または外部の他のボリュームへ一定セットのデータを転送する時に、ストレージシステムは転送の許可および／または変換を説明しているテーブルを捜す。もしもテーブルによって許可が認められるならば、ストレージコントローラはデータを変換し転送先にデータを転送する。もしも、例えば、システムがデフォルトとして“暗号化の後に許可”を設定すると、データがストレージシステムの制御の外に移動された後にさえも、秘密データの予期しない破壊は避けることができ、データは保護されることができる。
【発明の効果】
【００１７】
ストレージシステムが一つのボリュームから他のエリア、例えばホスト、テープストレージ、またはストレージシステム内部または外部の他のボリュームへ一定セットのデータを転送する時に、ストレージシステムは転送の許可および／または変換を説明しているテーブルを捜す。もしもテーブルによって許可が認められるならば、ストレージコントローラはデータを変換し転送先にデータを転送する。もしも、例えば、システムがデフォルトとして“暗号化の後に許可”を設定すると、データがストレージシステムの制御の外に移動された後にさえも、秘密データの予期しない破壊は避けることができ、データは保護されることができる。
【発明を実施するための最良の形態】
【００１８】
００１３　本発明のこれらおよび他の特徴と利点は好適な実施例の以下の詳細な説明を考慮してこの技術に通常程度に精通している人達に明かになるであろう。
【００１９】
００１４　上記の一般的な記述と共に、添付の図面と以下に提供される好適な実施例の詳細な記述は、本発明の今日考えられる最良な形での好適な実施例の原理を示し説明するために役に立つ。
【００２０】
００２６　本発明の以下の詳細な記述において、開示の一部を形成する添付の図面が参照されて、本発明が実施される場合の特定な実施例が説明のために示されるが、これに限定されることはない。図面において、同じ番号はいくつかの図を通して実質的に同様な構成部分を意味する。
【００２１】
システム構成
００２７　図１は本発明の基本的なシステム構成を示す。１０１は論理装置または論理ボリューム１０４、１０５、１０６を有し、データ保存場所として働き、および分割された単一のハードディスクドライブ、複数のハードディスクドライブ、ＲＡＩＤアレイ、または他の既知のストレージ装置のような物理的ストレージ装置として実現されることのできるストレージシステムである。ディスクコントローラ１１０はサーバからのボリューム上のデータの読み出しおよび書き込み要求を制御するために含まれる。システム１０１はまた暗号化／復号化、圧縮／解凍の機能を実行するコンバータ１０７を含み、またこれ

はソフトウエアモジュールまたはハードウエアアクセレレータとして実現される場合がある。システム１０１はさらに変換定義テーブル１０８を含み、これはデータ転送許可および変換要求に関する表示を有し、以下により詳細に説明される。システム１０１はまた暗号化および復号化のためのキーとアルゴリズムＩＤを少なくとも有するアルゴリズムＩＤテーブル１０９を含む場合がある。さらに、認証定義テーブル１１５はキー検索を要求する実体の確実性を確認する場合に使用するために備えられ、以下により詳細に説明される。さらに、ポート１０２、１０３はホスト接続のためにシステム１０１に含まれ、これによって、例えばサーバ１１２と１１４のような装置、ユーザ、ホスト等はそれぞれホストバスアダプタ（ＨＢＡ）１１１と１１３等を経由してストレージシステム１０１と接続される。

【００２２】

システムオペレーション

００２８　図２は図１の変換定義テーブル１０８の例を示す。テーブル１０８において、データ位置またはソース、指定の論理装置またはストレージシステム１０１のボリューム１０４、１０５、１０６は列２０１にリストされており、これはここでソースの装置またはボリュームと呼ばれ、列２０２はソースの装置またはボリューム１０４、１０５、１０６の状態を説明する。状態は非加工（Ｐ）、暗号化（Ｅ）、または圧縮（Ｃ）である。データが非加工の状態Ｐでない時には、暗号化または圧縮に情報を関連付けるためアルゴリズムＩＤが後に続く。圧縮の状態Ｃは非加工の状態Ｐと暗号化の状態Ｅの両方と結合される場合がある。

【００２３】

００２９　図３はアルゴリズムＩＤテーブル１０９の例を示す。テーブル１０９の第一の列３０１に示されるように、暗号化に対する各アルゴリズムＩＤ（アルゴリズムＩＤの３０２、３０５、３０６、３０７）は、テーブル１０９の“属性”の列３０８に指定されているように、ＤＥＳ、３ＤＥＳ、ＡＥＳ等のアルゴリズムのセット、ＥＣＢモード、ＣＢＣモード等のモード、およびキーと少なくとも関連する。暗号技術が進歩するとキーおよび／または暗号化アルゴリズムは更新される必要がある場合があるので、暗号化に対するアルゴリズムＩＤはまた、キーが生成される時点を特定する日付情報を有する場合がある。

【００２４】

００３０　図２に戻って、変換テーブル１０８は、列２０１の各ボリューム１０４－１０６が露出されるかもしれない、すなわちソースボリューム１０４－１０６上のデータがそれによって読み出され、コピーされ、または書き込まれる場合があるターゲット２０３－２０７を含む。さらに、テーブル１０８の各セルはデータがターゲットに露出される方法の状態およびデータ転送の可能な方向を有する。各セルにおける状態の表記は列２０２と同じである。

【００２５】

００３１　データ転送の可能な方向に関して、“Ｕ”は単一方向性、すなわちソースからターゲットへだけを表わし、“Ｂ”は双方向性、すなわちソースからターゲットおよびターゲットからソースを表わす。“ＮＡ”が特定されると、これはソースボリュームはターゲットによってアクセスされることを全く許されないことを意味する。もちろん、上記および図２と３で説明された表記は本発明の特定な実施例のフォーマットに関して異なる場合がある。

【００２６】

００３２　セル２１０と２１１を考慮すると、例えば、変換テーブル１０８の使用方法は以下のように説明される。ボリューム１０４上のデータは、状態の列２０２の“Ｐ”によって示されているように、状態が非加工である。もしもデータをボリューム１０４からボリューム１０５へ転送する要求が受け取られると、セル２１０の調査では、データが、図３のアルゴリズムＩＤテーブル１０９の項目番号３０２で特定されるように、アルゴリズムＩＤ　Ｋ１を有するアルゴリズムを使用して、暗号化（“Ｅ”で示されているよう

に）の後にボリューム１０５へコピーされることを許可されることを示す。また、セル２１０に示されている方向は、セル２１０内の“Ｂ”で示されているように、双方向性なので、ボリューム１０５上のデータはアルゴリズムＩＤ　Ｋ１を使用して復号化の後でボリューム１０４へコピーされることを許可される。従って、セル２１０と２１３は基本的に同じデータ転送を特定し、一致しなければならない。

【００２７】

００３３　他の例において、ボリューム１０５上のデータは、状態の列２０２に示されているように、アルゴリズムＩＤ　Ｋ１で暗号化される。テーブル１０８の列２０６、セル２１１に示されているように、ボリューム１０５上のデータはＨＢＡ１１１を経由してサーバ１１２によって読み出されることが許可される。ＨＢＡ（例えば、ＨＢＡ１１１、１１３）のＩＤがサーバ（例えば、サーバ１１２、１１４）のＩＤまたは名前の代わりにテーブル１０８において使用される理由は、ストレージシステムとサーバの間の認証が、従来技術では、ＨＢＡのＷＷＮ（ｗｏｒｌｄ　ｗｉｄｅ　ｎａｍｅ）を使用して実行されるからである。しかしながら、これは本特許を限定するものと解釈されるべきでない。もしもアプリケーションまたはユーザを特定するような技術が利用可能ならば、これはＨＢＡのＷＷＮ、サーバのなんらかのＩＤ、サーバ上で走行するアプリケーションのＩＤ、またはユーザのＩＤであることが可能であろう。

【００２８】

００３４　ＨＢＡに露出されたデータの状態が“Ｐ”であるので、サーバ１１２が見ることのできるデータは非加工フォーマットで転送されなければならない。従って、ボリューム１０５上のデータは暗号化されているので、データはＨＢＡ１１１とサーバ１１２への転送のためにアルゴリズムＩＤ　Ｋ１の復号化によって変換されなければならない。さらに、単一方向性がセル２１１の“Ｕ”によって特定されているので、サーバ１１２はデータをボリューム１０５上に書き込むことを許可されない。

【００２９】

００３５　他の例において、セル２１２は、どんなタイプのコミュニケーションが、もしあれば、ボリューム１０６とＨＢＡ１１１の間で起きることが可能かを示す。ボリューム１０６上のデータは非加工（Ｐ）の状態であり、ＨＢＡ１１１への転送の前に、セル２１２の“Ｅ”と“Ｋ４”によって示されているように、データはアルゴリズムＩＤ　Ｋ４で暗号化されなければならない。さらに、セル２１２の“Ｃ”と“Ｃ１”によって示されているように、データはアルゴリズムＩＤ　Ｃ１で圧縮されることを要求される。この事について、暗号化後の圧縮はより難しいので、暗号化の前にデータを圧縮することが望ましい。さらに、単一方向性がセル２１２の“Ｕ”によって特定されているので、データはボリューム１０６からＨＢＡ１１１（サーバ１１２）へだけ転送されることができるが、しかしサーバ１１２はＨＢＡ１１１を経由してボリューム１０６へデータを転送することはできない。

【００３０】

００３６　図４は、変換テーブル１０８をベースにＩ／Ｏ要求またはデータコピー要求に応じてボリューム１０４-１０６上のデータを転送する時に、図１のディスクコントローラ１１０が動作する方法の例を示すフローチャートである。ディスクコントローラ１１０がデータを転送することを通知された時に（ステップ４０１）、ディスクコントローラ１１０は変換定義テーブル１０８をチェックして転送パスを記述している変換定義テーブル１０８のセルを特定する（ステップ４０２）。もしもテーブルの調査が変換タイプはＮＡであることを示すならば（ステップ４０３）、ディスクコントローラ１１０は処理を終了する（ＥＮＤ）。もしもそうでないと、ディスクコントローラ１１０は転送の方向をチェックする（ステップ４０４）。もしも方向がソースからターゲットであると、ディスクコントローラ１１０はソースの状態とターゲットのそれが同じ、例えば、両方が非加工または両方が同じアルゴリズムＩＤで暗号化、であるかをチェックする（ステップ４０５）。もしも状態が同じであると、ディスクコントローラ１１０はソースからターゲットへデータを転送する（ステップ４０７）。もしもそれらが同じでないと、ディスクコントロ

ーラ１１０はソースの状態からターゲットの状態にデータを変換し（ステップ４０６）、次に変換されたデータをターゲットに転送する。

【００３１】

００３７　図２のセル２１０を考慮すると、例えば、ソースボリューム１０４の状態は非加工でありターゲットボリューム１０５の状態はアルゴリズムＩＤ　Ｋ１で暗号化されるので、ボリューム１０４上のデータは転送の前にアルゴリズムＩＤ　Ｋ１で暗号化される。一度データが変換されると、データはターゲットに転送される（図４のステップ４０７）。もしも転送の方向がターゲットからソースであり、方向が双方向でないと（ステップ４０８）、ディスクコントローラ１１０は転送を終了する（ＥＮＤ）。もしも転送の方向がターゲットからソースであり、方向が双方向であり（ステップ４０８）、ターゲットの状態とソースのそれが同じであると（ステップ４０９）、データはソースに転送される（ステップ４０７）。もしも状態が同じでないと、データは変換されて（ステップ４０６）次に転送される（ステップ４０７）。

【００３２】

００３８　図４は説明の目的のために簡単化されており、本発明の処理はストレージシステムのデータ転送メカニズムの実施形態に従ってカスタマイズされている。例えば、多量のデータがソースからターゲットに転送される時に、暗号化、復号化、およびデータ転送は、ブロックごとをベースとして処理される。すなわちデータ変換（ステップ４０６）とデータブロック転送（ステップ４０７）が全部のデータ転送が完了するまで繰り返される必要があるが、一方ステップ４０３、４０５、４０８および４０９などのチェック処理は一度だけ実行される必要がある。以下は、ソースの状態からターゲットの状態にステップ４０６においてデータの変換をすることに関してのいくつかの特記事項である。

【００３３】

００３９　一般的に、暗号化されたデータの圧縮比率は低くなるので、圧縮は暗号化の前に行われる。この理由のため、データが暗号化の前に圧縮されおよび復号化の後に解凍されることが特定される処理の順序については、ここでは省略される。しかし、もしもデータの状態の変換がいくつかの機能、例えば暗号化と圧縮の両方を含み、順序が暗黙的に定義されていなければ、これらの処理の順序はアルゴリズムＩＤテーブル１０９において明確に特定される必要が通常はある。

【００３４】

００４０　アルゴリズムＩＤはデータが圧縮または解凍される方法についての情報を有する。図３の項目３０３および３０４は圧縮アルゴリズムＩＤの例である。例えば、アルゴリズムＩＤ３０３はデータ全体がＺＩＰアルゴリズムを使用して圧縮または解凍されることを意味する。

【００３５】

００４１　データが圧縮される時に、システム１０１のコンバータ１０７はソース、ターゲット、または他の機能である入力から圧縮される全てのデータをロードし、次にＺＩＰアルゴリズムなどの特定の圧縮アルゴリズムを使用してデータを圧縮する。結果のデータは特定のパディングメカニズムを使用してパディングされる。アルゴリズムＩＤ３０３において、結果のデータの長さは５１２バイトのブロックサイズのようなＳＣＳＩプロトコルで共通的に使用されるブロックサイズで割り切れない場合があるので、パディングメカニズムが使用される。例えば、データをパディングするためのＩＳＯ／ＩＥＣ９７９７－１Ｍｅｔｈｏｄ２において、メッセージは一つの１を付加されて次にメッセージの長さをｎで割り切れるようにするために必要な数の０を付加する。最後の１はメッセージの最終のマーカとして作用する。パディングされたデータは行先に転送され、これはソース、ターゲットまたは暗号化のような他の機能である。

【００３６】

００４２　データが解凍される時に、コンバータ１０７はソース、ターゲット、または復号化のような他の機能である入力から解凍されるべき全てのデータをロードする。次にコンバータ１０７はパディングメカニズムに従ってパディングデータを取り除く。結果

のデータは次にＺＩＰアルゴリズムのような特定のアルゴリズムを使用して解凍され、行先に転送される、これはソース、ターゲットまたは他の機能である。

【００３７】

００４３　ボリューム１０６上の全部のデータのサイズがサーバ１１２によって問われる時に、圧縮されたデータのサイズはコンバータ１０７によって計算され、サーバ１１２に戻される。このサイズは変換定義テーブル１０８に追加のフィールド（示されていない）として記録されるであろう。ボリューム１０６上のデータが更新される時に、サイズは再計算されるであろう。さらに、ボリュームデータの一定の領域だけがしばしば更新されることが知られている時に、データの全体をいくつかの部分に分割して、各部分のサイズを計算することが有益である。ボリューム上のデータが問われる時に、各部分のサイズの合計が計算されて次にサーバに戻され、これは計算時間を短縮する。

【００３８】

００４４　図３のアルゴリズムＩＤ３０４は分割されたデータを圧縮するための例である。ソースボリュームのデータ全体が１Ｍバイトまたはより小さいデータに分割されて、各部分が、属性の列３０８に示されるように、ＬＨＡアルゴリズムを使用して圧縮される。結果のデータはＩＳＯ／ＩＥＣ９７９７－１Ｍｅｔｈｏｄ３を使用してパディングされ、これは圧縮前のデータの長さを圧縮されたデータの前に明確に加算する。データをパディングするためのＩＳＯ／ＩＥＣ９７９７－１Ｍｅｔｈｏｄ３において、メッセージはメッセージの長さがｎで割り切れるまでゼロを付加され、次に追加のブロックが、元のメッセージの長さを有するデータの流れの前に追加される（完全なブロックするために左にゼロをパディングする）。このアルゴリズムが使用される時に、データの更新された部分だけのサイズが計算される必要がある。

【００３９】

００４５　図２に示されるように、ボリューム１０５上のデータが変換定義テーブル１０８のセル２１４をベースにＨＢＡ１１３を経由してサーバ１１４に転送される時に、データがサーバ１１４に転送される前に、ボリューム１０５上のデータは最初アルゴリズムＩＤ　Ｋ１で復号化されて（列２０２のボリューム１０５の状態によって示されるように）、次にアルゴリズムＩＤ　Ｋ２で暗号化される（セル２１４のボリューム１０５に関係するＨＢＡ１１３の状態によって示されるように）。

【００４０】

００４６　データを暗号化および復号化するキーはストレージシステム１０１の内部で生成される。アクセスが適切に認証されなければ、それらはストレージシステム１０１から出ない。キーはアルゴリズムＩＤテーブル１０９上に保存され、これは一つ以上のアルゴリズムＩＤを有する。キー検索のプロトコルはＨｔｔｐｓ、ファイバチャネルネットワーク、または他のネットワークプロトコルなどのＩＰネットワーク上で実施される場合がある。図１に示されるように、インタフェース１１６はキーを検索するために管理サーバ１１７がストレージシステム１０１とインタフェース動作を行うために使用されるインタフェースである。

【００４１】

００４７　図６に示されるように、認証定義テーブル１１５はキー検索を要求する実体の確実性を検証するために使用される。アルゴリズムＩＤテーブル１０９、変換定義テーブル１０８および認証定義テーブル１１５は、暗号化またはパスワード保護のような適切な保護方法で、ＩＣカード、ＰＣ等のようなストレージシステム１０１の外部の領域に確実にバックアップされることができる。

【００４２】

００４８　変換定義テーブル１０８と認証定義テーブル１１５を構成するための特権はこれらのテーブルに加えて定義される必要がある。現在の技術（例えば、ＵＮＩＸ（登録商標）ＮによるＡＣＬのような）はこれらのテーブルへのアクセスを制御するために使用することができる。ボリュームがストレージシステム１０１に生成される時に、またはその後のある時に、構成処理が行われる場合がある。構成処理はまた、データを露出する

新しいパスが追加される時に、例えば、ホストに接続された新しいポートが追加されるか、または新しい遠隔コピーのペアが生成される時に、またはその後のどこかの時点で、実行される場合がある。

【００４３】

００４９　本発明の目的がより良く理解されるために、本発明が実施される具体例のシナリオがここで説明される。アプリケーションがサーバ１１２上で走行しており、ボリューム１０４上のデータの読み出しおよび書き込みをしている。ボリューム１０４上のデータはボリューム１０５に複製される。ストレージ管理者はサーバ１１４にログオンして、ボリューム生成またはボリューム１０４からボリューム１０５への複製の構成処理のようなストレージ管理を行う。

【００４４】

００５０　ボリューム１０４上のデータはサーバ１１２上から見られることを許可される、何故ならばサーバ１１２上のアプリケーションはデータを読み出し、処理し、および書き込む必要があるからである。サーバ１１４にログオンしているストレージ管理者はボリューム１０４からボリューム１０５への複製を構成するためにボリューム１０４とボリューム１０５にアクセスする必要があるが、しかしボリューム１０４とボリューム１０５上のデータの内容を理解する必要はない。

【００４５】

００５１　本発明を使用して、ボリューム１０４上のデータは実際には暗号化されないが、ストレージ管理者はボリューム１０４をアクセスすることができ、暗号化されたデータを読み出すことができる。ボリューム１０４上のデータは、ボリューム１０４から出る時に暗号化される。ストレージ管理者はデータを復号化および暗号化するためのキーを有していないので、ストレージ管理者によるボリューム１０４上の書き込みはデータの一貫性を保持するために許可されない。

【００４６】

００５２　他の代表的なシナリオにおいて、データは、図５に示されているように、ボリューム１０４のようなボリュームからテープ５０１にコピーされる。サーバ１１４は、テープ５０１上にデータを書き込む前に、ボリューム１０４上のデータを暗号化することができる場合があるが、しかしサーバ１１４は、ストレージシステム１０１内の全てのデータの安全性に対して責任があり、テープ上に書き込む前に暗号化を構成することを忘れる場合があるストレージ管理者以外の人によってたぶん管理されるであろう。もちろん、もしもデータがなんらかの暗号化無しでサーバ１１４に転送されると、これは安全ではない場合がある。本発明を使用して、しかし、ストレージシステム１０１を出るデータはセル２１５の変換要求に従って暗号化されるように構成されることができ、従ってデータの秘密性の管理は集中化される。

【００４７】

００５３　さらに他の代表的なシナリオにおいて、図７に示されるように、ボリューム１０６からのデータは遠隔コピーインタフェース７０２と７０３を経由して遠隔ストレージシステム７０１内の遠隔ボリューム７０４にコピーされる。ストレージシステム７０１はサードパーティの組織によって管理される場合があり、ボリューム７０４に転送されるデータは保護される必要がある場合がある。このようなケースでは、ボリューム１０６上のデータは図８のテーブル１０８ａのような変換定義テーブルをベースにボリューム７０４にコピーされる前に暗号化されることができる。遠隔ボリューム７０４にコピーされるデータは、ボリューム１０６上のデータが壊れるケースでは、ボリューム１０６に戻される場合がある。このようなケースでは、遠隔ボリューム７０４上のデータはストレージシステム１０１にコピーされ、アルゴリズムＩＤ　Ｋ２で復号化され、次にボリューム１０６に書き込まれる。

【００４８】

００５４　予期しない安全性の破壊を避けるために、管理者による明確な構成処理なしにだれも非加工（Ｐ）データを見ることができないように、ストレージシステムのユー

ザが自動的に変換テーブル１０８を生成することは有益である。例えば、明確な定義がないと、ボリューム上のデータが盗まれないように、各セルはＮＡまたは”（Ｅ，Ｋｘ），（Ｕ）“の状態に設定されることができ、すなわちもしもそれがなんらかで盗まれても、暗号化されている。

【００４９】

００５５　ボリューム１０４上のデータがサーバ１１４にログオンしている一定のユーザに暗号化されているフォームで露出される時に、もしもユーザが暗号化に使用されるアルゴリズムＩＤ情報を検索することを許可されていると、安全性がない。ディスクコントローラ１１０は変換定義テーブル１０８と認証定義テーブル１１５を比較することによってそのような問題を検出する機能を有することができる。

【００５０】

００５６　暗号化されたデータが長い時間の間保存されている時に、キーと暗号化アルゴリズムは更新される必要がある。このようなケースでは、再キー設定処理が行われる。図９はボリューム１０５のようなボリューム上の再キー設定に対して使用される変換定義テーブル１０８ｂを示す。

【００５１】

００５７　最初に、ターゲットに露出されるデータとデータ転送の方向の状態はセル１００１に挿入され、これはそうでないと通常は空欄である。この動作はできれば、管理サーバ１１７によってのように、ストレージシステム１０１の外から指示される。実際にデータ転送の方向はここでは何らかの意味もない。この例で、ボリューム１０５上のデータに対するアルゴリズムＩＤはＫ１からＫ３に変更される。次に、ディスクコントローラ１１０はブロックごとにデータを読み出し、アルゴリズムＩＤ　Ｋ１とＫ３を使用してデータを変換する。大部分の従来の暗号化アルゴリズムは暗号化の後にデータの長さを変えないし、変換されたブロックはそれが読み出されたのとまったく同じ位置に書き込まれる。このブロックごとの処理はボリューム１０５の全部のデータの変換が完了するまで繰り返えされる。変換が完了すると、列２０２のボリュームの状態はセル１００１の状態で上書きされ、次にセル１００１は空欄に設定される。ディスクコントローラ１１０は、データがすでに変換されているかどうかの情報を保持することによって適切なアルゴリズムＩＤを特定できるので、許可されている時に、変換の間にボリュームに入ってくるＩ／Ｏを受け取ることができる。もちろん、非加工データを暗号化にまたは暗号化を非加工に変換することも可能である。

【００５２】

００５８　ボリュームレベルの変換が上記で説明されるが、しかし、明かに、この技術はファイルレベルの変換に拡大されることができる。このようなケースで、変換定義テーブル１０８および認証定義テーブル１１５のエントリはボリュームではなくファイルになる。

【００５３】

００５９　本発明はどんな変換も処理できる。例えば、暗号化／復号化が上記の説明において仮定されているが、暗号化／復号化無しの圧縮だけが処理されることができる。もしもＳＨＡ－１、またはｍｄ５のような片道機能が特定されると、変換定義テーブル１０８上で特定される方向は単一方向性であろう。

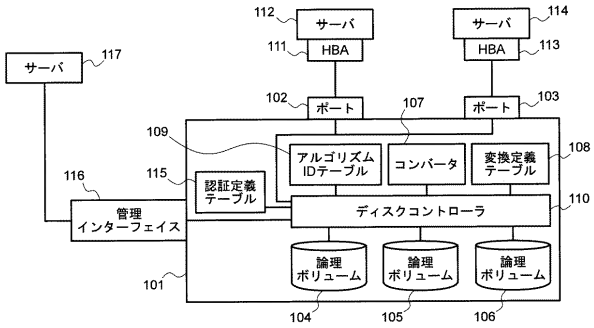
【００５４】

００６０　図１０と１１はデータが転送の前に１０ＧＢから５ＧＢに最初に圧縮される他の実施例を示す。しかし、データの正しいサイズが求められるまで転送は起きることができない。図１１のステップ６１０に示されるように、データは変換定義テーブルで要求されるように圧縮される。ステップ６１１で、データオーバフローがあるかが決定される。言い換えると、データの求められるサイズがデータの実際のサイズに一致するかが決定される。もしもそうならば、特定された長さのデータが戻される（ステップ６１２）。もしもそうでないと、処理は終了する（ステップ６１３）。データが転送されない時の例は５ＧＢのデータから１０ＧＢのデータを読み出す試みをした時である。他の例はボリュ

ームの最後から５１２バイトを読み出す試みである。
【００５５】
００６１　特定の実施例がこの明細書に示され説明されたが、この技術に通常程度に精通している人達は、同じ目的を達成するために意図されるどんな調整も開示された特定の実施例に対して置き換えられることができることを十分に認識する。従って、この開示内容は本発明の任意のおよび全ての適応または変化も含むことを意図しており、上記の説明内容は限定的ではなく、説明的な形式でなされたことを理解すべきである。構造的なおよび論理的な置き換えおよび変更が本発明の範囲から離れることなく行われることができるように、他の実施例が活用されそこから引き出されることができる。本発明の範囲は添付の請求項に関して、この請求項が与えられる同等内容の全範囲と共に、適切に決定されるべきである。
【図面の簡単な説明】
【００５６】
【図１】図１は本発明の基本的なシステム構成を示す。
【図２】図２は本発明の変換テーブルの例を示す。
【図３】図３は本発明のアルゴリズムＩＤテーブルの例を示す。
【図４】図４はディスクコントローラが変換テーブルをベースにＩ／Ｏ要求またはデータコピー要求に応じてボリューム上のデータを転送する方法の一例を説明するフローチャートである。
【図５】図５はボリュームからテープへデータをコピーするための本発明のシステムを示す。
【図６】図６は本発明の認証定義テーブルを示す。
【図７】図７はローカルボリュームから遠隔ボリュームへのデータの遠隔コピーのための本発明のシステムを示す。
【図８】図８は図７の実施例で使用するための本発明の変換定義テーブルを示す。
【図９】図９はボリューム上のデータの再キーに使用される変換定義テーブルを示す。
【図１０】図１０は転送時のデータ圧縮を示す。
【図１１】図１１は圧縮データがアドレスのオーバフロに対してチェックされる本発明の実施例のフローチャートを示す。
【符号の説明】
【００５７】
１０２　ポート
１０３　ポート
１０４　論理ボリューム
１０５　論理ボリューム
１０６　論理ボリューム
１０７　コンバータ
１０８　変換定義テーブル
１０９　アルゴリズムＩＤテーブル
１１０　ディスクコントローラ
１１１　ＨＢＡ
１１２　サーバ
１１３　ＨＢＡ
１１４　サーバ
１１５　認証定義テーブル
１１６　管理インタフェース
１１７　サーバ

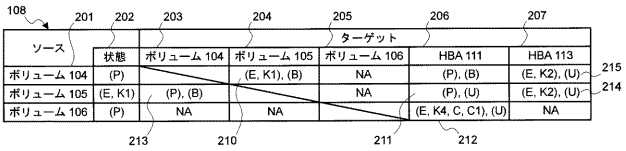
【図１】

図１




【図２】

図２



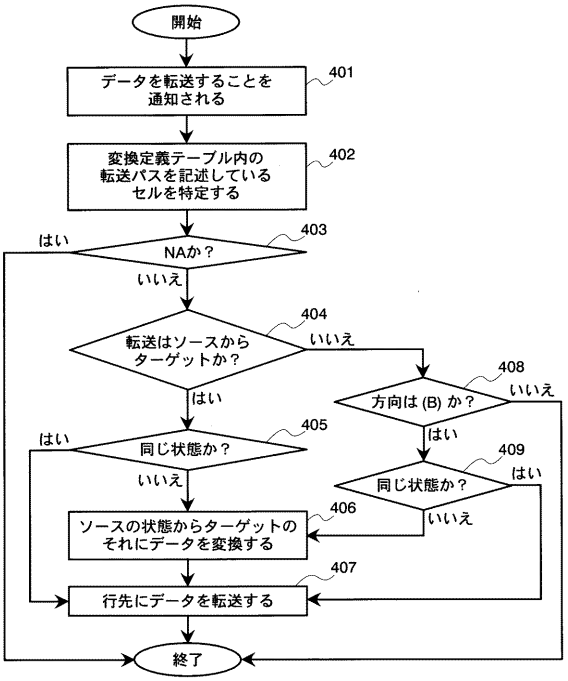

【図３】

図３

| アルゴリズムID | 属性 |
|---|---|
| K1 | DES, ECB Mode, 0x1234567812345678 |
| K2 | DES, ECB Mode, 0x8765432187654321 |
| K3 | 3DES, ECB Mode, 0x1234567812345678, 0x8765432187654321 |
| K4 | DES, ECB Mode, 0xabcdefabcdefabcd |
| C1 | ZIP, Whole Data, ISO/IEC 9797-1 method 2 |
| C2 | LHA, 1 M Bytes, ISO/IEC 9797-1 method 3 |

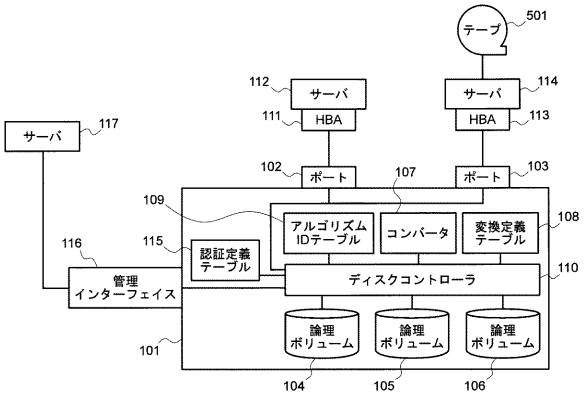
【図４】

図４




【図５】

図５



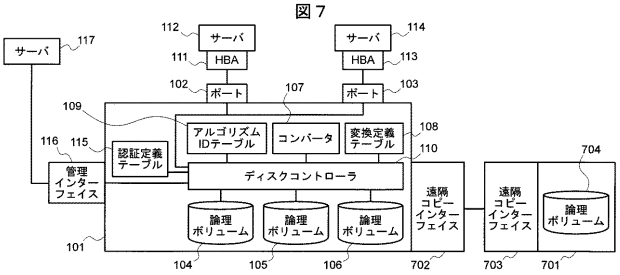

【図６】

図６

| アルゴリズムID | ユーザID | パスワード |
|---|---|---|
| K1 | HBA 111 | abcdef |
| K2 | HBA 111 | 012345 |
| K3 | 管理者 | 9876543210 |
| K4 | | |

【図７】

図７




【図８】

図８

| ソース | 状態 | ターゲット ボリューム 104 | ボリューム 105 | ボリューム 106 | HBA 111 | HBA 113 | 702, 703経由のボリューム704 |
|---|---|---|---|---|---|---|---|
| ボリューム 104 | (P) | | (E, K1), (B) | NA | (P), (B) | (E, K2),(U) | NA |
| ボリューム 105 | (E, K1) | (P), (B) | | NA | (P), (U) | (E, K2),(U) | NA |
| ボリューム 106 | (P) | NA | NA | | (E, K4, C, C1), (U) | NA | (E, K2), (B) |

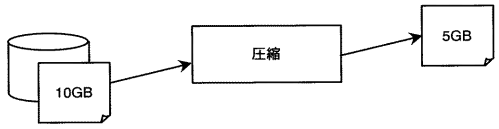
【図９】

図９

| ソース | 状態 | ターゲット ボリューム 104 | ボリューム 105 | ボリューム 106 | HBA 111 | HBA 113 |
|---|---|---|---|---|---|---|
| ボリューム 104 | (P) | | (E, K1), (B) | NA | (P), (B) | (E, K2), (U) |
| ボリューム 105 | (E, K1) | (P), (B) | (E, K3), (-) | NA | (P), (U) | (E, K2), (U) |
| ボリューム 106 | (P) | NA | NA | | (E, K4, C, C1), (U) | NA |

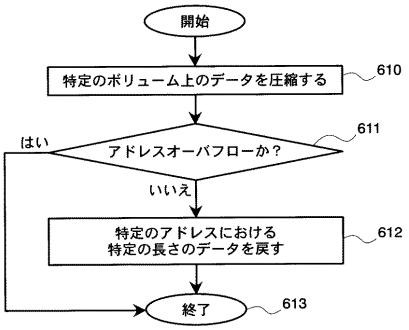
【図１０】

図１０




【図１１】

図１１



【外国語明細書】
2006114029000001.pdf