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

特許第4382328号
(P4382328)

(45)発行日　平成21年12月9日(2009.12.9)　(24)登録日　平成21年10月2日(2009.10.2)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520B
G06F 12/00	(2006.01)	G06F	12/14	530C
G06F 3/06	(2006.01)	G06F	12/00	537A
		G06F	12/00	501A
		G06F	12/00	514E

請求項の数 16　(全 30 頁)　最終頁に続く

(21)出願番号　特願2002-169725 (P2002-169725)
(22)出願日　平成14年6月11日 (2002.6.11)
(65)公開番号　特開2004-13778 (P2004-13778A)
(43)公開日　平成16年1月15日 (2004.1.15)
審査請求日　平成17年3月14日 (2005.3.14)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100084537
弁理士　松田　嘉夫
(74)代理人　100114236
弁理士　藤井　正弘
(72)発明者　木谷　誠
東京都国分寺市東恋ヶ窪一丁目２８０番地
株式会社日立製作所　中央研究所内
(72)発明者　星野　和義
東京都国分寺市東恋ヶ窪一丁目２８０番地
株式会社日立製作所　中央研究所内
最終頁に続く

(54)【発明の名称】セキュアストレージシステム

(57)【特許請求の範囲】
【請求項１】
ストレージ及び前記ストレージを使用し、仮想閉域網に接続されたクライアントによって構成されるストレージシステムであって、
前記ストレージに設定された論理ボリューム、前記論理ボリューム内のアドレス範囲及び前記仮想閉域網を、前記クライアントに割り当てる管理装置と、
前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換する変換装置と、
前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とを対応付けて記憶したマッピング手段と、を備え、
前記変換装置は、前記マッピング手段に記憶された対応付けに基づいて、仮想閉域網からのクライアントの要求をストレージの接続に用いるプロトコルに変換することを特徴とするストレージシステム。
【請求項２】
前記マッピング手段は、前記仮想閉域網の識別情報と、前記ストレージに設定された論理ボリュームのアドレス範囲及び前記論理ボリュームを有するストレージの識別情報との対応を規定するエントリを記憶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】

前記管理装置は、
前記クライアント、前記変換装置間の仮想閉域網を前記仮想閉域網識別情報を使用して設定する仮想閉域網設定手段と、
前記変換装置、前記ストレージ及び前記仮想閉域網を管理する仮想閉域網管理手段と、
前記クライアントが前記ストレージを使用するときに、前記クライアントに割り当てられた仮想閉域網と、該仮想閉域網に対応する前記ストレージのアクセス範囲との対応を、前記マッピング手段に記憶させるエントリ設定手段と、を備えることを特徴とする請求項１又は２に記載のストレージシステム。
【請求項４】
前記仮想閉域網識別情報を使用して仮想閉域網を設定するネットワーク制御装置を備え、
前記管理装置は、前記仮想閉域網識別情報を使用した仮想閉域網を前記ネットワーク制御装置に設定させる仮想閉域網設定要求手段を備え、
前記ネットワーク制御装置は、前記仮想閉域網設定要求手段からの要求に従って、複数ネットワークにわたる前記仮想閉域網を設定することを特徴とする請求項１から３のいずれか一つに記載のストレージシステム。
【請求項５】
前記ネットワーク制御装置は、前記仮想閉域網識別情報を有するトラフィックに対する通信品質を設定し、該仮想閉域網の通信品質を保証す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６】
前記クライアントは、前記管理装置から送信された、前記変換装置の識別情報と仮想閉域網識別情報を使用して、該仮想閉域網によって前記変換装置まで接続し、
前記管理装置は、前記クライアントを認証し、この認証結果に基づいて、前記変換装置に前記クライアントと同じ仮想閉域網識別情報による仮想閉域網を設定し、
前記クライアントは、前記設定された仮想閉域網を用いて前記ストレージへ接続することを特徴とする請求項１から５のいずれか一つに記載のストレージシステム。
【請求項７】
前記ストレージに設定された論理ボリュームに記憶される情報を予備的に記憶するバックアップストレージと、
前記バックアップストレージに対するプロトコルと前記仮想閉域網で使用されるプロトコルとを変換するバックアップ変換装置と、を備え、
前記管理装置は、前記クライアントが前記論理ボリュームを使用するときに、前記バックアップ変換装置の識別情報を前記マッピング手段に記憶させるバックアップエントリ設定手段を備えることを特徴とする請求項１から６のいずれか一つに記載のストレージシステム。
【請求項８】
前記ストレージに障害が発生した場合は、前記クライアントと前記論理ボリュームとの間で前記変換装置が転送するデータを、前記変換装置が前記バックアップ変換装置を介して前記前記クライアントと前記バックアップストレージとの間で転送するデータ転送手段を備えることを特徴とする請求項７に記載のストレージシステム。
【請求項９】
前記管理装置は、単一又は複数の論理ボリュームから構成される仮想ボリュームを生成する仮想ボリューム生成手段を備え、
前記マッピング手段は、前記仮想ボリュームのアドレスを前記論理ボリュームのアドレスに変換するオフセットアドレスを記憶し、
前記変換装置は、前記仮想ボリュームのアドレスと前記マッピング手段で記憶したオフセットアドレスとを利用して、前記仮想ボリュームのアドレスを前記論理ボリュームのアドレスに変換するアドレス変換手段を備えることを特徴とする請求項１から８のいずれか一つに記載のストレージシステム。

【請求項１０】
ストレージに接続される変換装置であって、
前記ストレージを使用するクライアントと仮想閉域網によって接続され、
前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換するプロトコル変換手段と、
前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とを対応付けて記憶したマッピング手段と、を備えたことを特徴とする変換装置。
【請求項１１】
前記マッピング手段は、前記仮想閉域網識別情報と、前記ストレージに設定された論理ボリュームのアドレス範囲及び前記論理ボリュームを有するストレージの識別情報との対応を規定するエントリを記憶することを特徴とする請求項１０に記載の変換装置。
【請求項１２】
前記ストレージに設定された論理ボリュームに記憶される情報を予備的に記憶するバックアップストレージに対するプロトコルと前記仮想閉域網で使用されるプロトコルとを変換するバックアップ変換装置に接続され、
前記ストレージに障害が発生した場合には、前記ストレージとの間で転送されるべきデータを、前記バックアップ変換装置との間で転送するデータ転送手段を備えることを特徴とする請求項１０又は１１に記載の変換装置。
【請求項１３】
ストレージと、
仮想閉域網に接続されたクライアントと、
前記クライアントと前記仮想閉域網によって接続され、前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換する変換装置とで構成されるストレージシステムに用いられるストレージアクセス方法であって、
前記変換装置は、前記クライアントからの前記仮想閉域網を経由したアクセス要求を受信すると、前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とが対応付けられたマッピング情報を参照し、前記アクセス要求に含まれる仮想閉域網の識別情報が前記マッピング情報の仮想閉域網の識別情報と一致し、前記アクセス要求に含まれるアクセス範囲が前記マッピング情報のアクセス範囲内にあった場合に、前記変換装置に接続されている前記ストレージにデータを書き込み、
前記ストレージから書込終了の応答を受信すると、前記クライアントへ書込終了の応答を返信して、前記クライアントからのデータの書込処理を終了することを特徴とするストレージアクセス方法。
【請求項１４】
ストレージと、
仮想閉域網に接続されたクライアントと、
前記クライアントと前記仮想閉域網によって接続され、前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換する変換装置と、
前記変換装置とバックアップストレージとに接続され、前記バックアップストレージとの間の接続に使用されるプロトコルと前記変換装置との間で使用されるプロトコルとを変換するバックアップ変換装置とで構成されるストレージシステムに用いられるストレージアクセス方法であって、
前記変換装置は、前記クライアントからの前記仮想閉域網を経由したアクセス要求を受信すると、前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とが対応付けられたマッピング情報を参照し、前記アクセス要求に含まれる仮想閉域網の識別情報が前記マッピン

グ情報の仮想閉域網の識別情報と一致し、前記アクセス要求に含まれるアクセス範囲が前記マッピング情報のアクセス範囲内にあった場合に、前記変換テーブルに設定されている前記バックアップ変換装置へアクセス要求を送信し、
前記変換装置に接続されている前記ストレージにデータを書き込み、
前記ストレージから書込終了の応答を受信すると、前記クライアントへ書込終了の応答を返信し、
前記バックアップ変換装置は、前記変換装置からのアクセス要求を受信すると、前記仮想閉域網の識別情報の照合結果に基づいて、前記バックアップ変換装置に接続されているバックアップストレージにデータを書き込み、前記バックアップストレージから書込終了の応答を受信すると、前記変換装置へ書込終了の応答を返信し、
前記変換装置は前記バックアップ変換装置からの応答を受信すると、前記クライアントからのデータの書込処理を終了することを特徴とするストレージアクセス方法。

【請求項１５】
ストレージと、
仮想閉域網に接続されたクライアントと、
前記クライアントと前記仮想閉域網によって接続され、前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換する変換装置と、
前記変換装置とバックアップストレージとに接続され、前記バックアップストレージとの間の接続に使用されるプロトコルと前記変換装置との間で使用されるプロトコルとを変換するバックアップ変換装置とで構成されるストレージシステムに用いられる
ストレージアクセス方法であって、
前記変換装置は、前記クライアントからの前記仮想閉域網を経由したアクセス要求を受信すると、前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とが対応付けられたマッピング情報を参照し、前記アクセス要求に含まれる仮想閉域網の識別情報が前記マッピング情報の仮想閉域網の識別情報と一致し、前記アクセス要求に含まれるアクセス範囲が前記マッピング情報のアクセス範囲内にあった場合に、前記変換装置に接続されている前記ストレージへデータの読み込み要求を送信し、
前記ストレージからのデータを受信できないと、前記変換装置に接続されている前記バックアップ変換装置へアクセス要求を送信し、
前記バックアップ変換装置は、前記変換装置からのアクセス要求を受信すると、前記仮想閉域網の識別情報の照合結果に基づいて、前記バックアップ変換装置に接続されているバックアップストレージからデータを読み込み、前記バックアップストレージからのデータを受信すると、前記バックアップストレージからのデータを前記変換装置へ送信し、
前記変換装置は、前記バックアップ変換装置からのデータを受信すると、前記バックアップストレージからのデータを前記クライアントへ送信することを特徴とするストレージアクセス方法。

【請求項１６】
前記変換装置には、前記ストレージに設定された論理ボリュームによって前記ストレージを管理する管理装置が接続されて構成されるストレージシステムに用いられるストレージアクセス方法であって、
前記変換装置は、前記ストレージからのデータを受信できない場合に、前記管理装置に前記ストレージの障害情報を送信し、
前記管理装置は、前記ストレージの論理ボリュームの設定を変更することを特徴とする請求項１５に記載のストレージアクセス方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、クライアントとストレージがネットワークを介して接続されるストレージシス

テムに関する。
【０００２】
【従来の技術】
クライアントとストレージがネットワークを介して接続されるストレージシステムとしては、ＳＡＮ（Storage Area Network）が知られている。ＳＡＮはＦＣ（Fiber Channel）プロトコルで通信を行うＳＡＮファブリックによって構成され、クライアントはＳＣＳＩ（Small Computer Systems Interface）コマンドを用いてストレージにアクセスする。このようなＳＡＮの構成は、例えば、ＯＳＢＯＲＮＥ社２００１年発行の「Building Storage Networks SECOND EDITION」（ISBN 0-07-213072-5）（pp.23-30）に記載されている。
【０００３】
ＳＡＮではアクセス権を持たないクライアントからの不正アクセスを防止するために、図２７に示すようなゾーニング機能を用いてストレージ１１内の論理ボリューム１３とＦＣポート１２とをマッピングする。論理ボリューム１３とＦＣポート１２とのマッピングによって、ＦＣポート１２に接続を許可されたクライアント２１のみが論理ボリューム１３に対してアクセスが可能になり、ＦＣポート１２に接続していないクライアント２２は論理ボリューム１３にはアクセスできない。
【０００４】
ネットワークとしては、ＬＡＮ（Local Area Network）／ＭＡＮ（Metropolitan Area Network）／ＷＡＮ（Wide Area Network）が知られており、これらは、Ethernet（登録商標、以下同じ）、ＡＴＭ（Asynchronous Transfer Mode）、ＩＰ（Internet Protocol）などのネットワークプロトコルが広く用いられている。ＬＡＮ／ＭＡＮ／ＷＡＮに直接又はＳＡＮを経由して接続されたストレージへのアクセスには、ｉＳＣＳＩが知られている。ｉＳＣＳＩはネットワークプロトコル上でＳＣＳＩ命令を交換するプロトコルで、ストレージにブロック単位でアクセスすることができる。ｉＳＣＳＩの詳細はＩＥＴＦ発行の「ｉＳＣＳＩ」（dr aft-ietf-ips-iscsi）に記載されている。
【０００５】
ｉＳＣＳＩでは、不正アクセスを防止するために、ログイン認証に関するプロトコルが規定されているが、ＬＡＮ／ＭＡＮ／ＷＡＮの通信経路上でのデータの保護に関しては規定されていない。ＬＡＮ／ＭＡＮ／ＷＡＮでは、不特定多数のクライアントがネットワークに接続しているので、不正アクセス防止や盗聴防止などのセキュリティ対策が必要となる。この不正アクセスや盗聴を防ぐ手段としてはＶＰＮ（Virtual Private Network）が知られている。
【０００６】
ＶＰＮは、ＬＡＮ内で用いられているプライベートネットワークを構成するネットワークプロトコルを、ＬＡＮ／ＭＡＮ／ＷＡＮで用いられている別のネットワークプロトコルのペイロード部分に載せることで、遠隔地のプライベートネットワーク間を仮想的に１つのプライベートネットワークのエリアにする技術である。このＶＰＮをＬＡＮ／ＭＡＮ／ＷＡＮ上に設定することで、当該ＶＰＮ上のトラフィックをそれ以外のトラフィックから区別できるようになる。その結果、当該ＶＰＮ上の端末以外からの不正アクセスや盗聴を防止し、セキュリティを確保することができる。ＶＰＮには、ネットワークプロトコルごとに異なる種類が存在する。異なる種類のＶＰＮには接続性はなく、また同じ種類であってもＶＰＮを管理しているドメインが異なると接続が困難になる。そのため、統一された識別子であるＶＰＮ－ＩＤを使用することが提案されている。ＶＰＮ－ＩＤの詳細は、ＩＥＴＦ発行の「Virtual Private Networks Identifier」（ＲＦＣ２６８５）に記載されている。
【０００７】
ｉＳＣＳＩには、ＬＡＮ／ＭＡＮ／ＷＡＮの通信経路上でのデータの保護方式の一例としてＩＰＳｅｃがある。ＩＰＳｅｃは、認証又は暗号化のアルゴリズム若しくは鍵管理の仕組みをプロトコル自体から切り離し、さまざまなアルゴリズムをサポートすることができるように規定されている。そのため複数のプロトコルから構成される。ＩＰＳｅｃのセキ

ュリティの特徴はデータの改ざん及び漏洩の防止である。ＩＰＳｅｃは、接続元と接続先とのクライアントがＩＰＳｅｃに対応していて、かつ中継するネットワークがＩＰをサポートしていれば通信を確立することができる。そのため特別な装置が必要でなく適用範囲が広いという利点がある。ＩＰＳｅｃのセキュリティを使用し、ｉＳＣＳＩに認証を行わせることで、クライアントはＬＡＮ／ＭＡＮ／ＷＡＮを介してストレージにセキュアにアクセスすることができる。ＩＰＳｅｃのアーキテクチャの詳細は、ＩＥＴＦ発行の「Security Architecture for the Internet Protocol」（ＲＦＣ２４０１）に記載されている。

【０００８】

また、ストレージの論理ボリュームの数はＳＡＮのゾーニング機能によってＦＣポートの数に制限されるが、実際にはストレージを利用するクライアント数が少ないため運営上の問題は少ない。

【０００９】

【発明が解決しようとする課題】

しかしながら、上記従来技術には以下の問題がある。

【００１０】

クライアントがＬＡＮ／ＭＡＮ／ＷＡＮを介してストレージにアクセスするときは、ＳＡＮとＬＡＮ／ＭＡＮ／ＷＡＮでセキュリティを確保する必要がある。ＳＡＮではゾーニング機能によりセキュリティを確保することができ、ＬＡＮ／ＭＡＮ／ＷＡＮではｉＳＣＳＩと通信路上のデータ保護方式との組合せによってセキュリティを確保することができる。しかし、ＩＰＳｅｃには「なりすまし」を防止することができないという問題があり、どのようなネットワーク環境でも万能というわけではない。特にクライアントがストレージにアクセスするときに経由するネットワークのセキュリティや回線品質の保証ができない広域からのアクセスの場合、それぞれのネットワークに適したデータ保護方式を使用しなければ、より安全で確実なストレージへのアクセスをクライアントに提供することができない。そのため、ＶＰＮは単一の種類による構成だけでなく、複数の種類から構成される必要がある。

【００１１】

また、クライアントがＬＡＮ／ＭＡＮ／ＷＡＮを介してストレージにアクセスするとクライアント毎にボリュームを割り当てる必要がある。ｉＳＣＳＩでは１つのＦＣポートを複数のクライアントにアクセスさせることはできるが、クライアントごとに論理ボリュームを割り当てる機能はない。そのため、クライアントの接続数のスケーラビリティを向上させることはできても、論理ボリューム数のスケーラビリティの向上には問題が残る。

【００１２】

【課題を解決するための手段】

上記の課題を解決するために、本発明では、ストレージ及び前記ストレージを使用し、仮想閉域網に接続されたクライアントによって構成されるストレージシステムであって、前記ストレージに設定された論理ボリューム、前記論理ボリューム内のアドレス範囲及び前記仮想閉域網を、前記クライアントに割り当てる管理装置と、前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換する変換装置と、前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とを対応付けて記憶したマッピング手段と、前記マッピング手段に記憶された対応付けに基づいて、仮想閉域網からのクライアントの要求をストレージの接続に用いるプロトコルに変換するプロトコル変換手段と、を備えたことを特徴とする。

【００１３】

また、ストレージに接続される変換装置であって、前記ストレージを使用するクライアントと仮想閉域網によって接続され、前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網で使用されるプロトコルとを変換するプロトコル変換手段と、前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記スト

レージの前記論理ボリューム内のアクセス範囲とを対応付けて記憶したマッピング手段と、を備えたことを特徴とする。

【００１４】

また、ストレージと、仮想閉域網に接続されたクライアントと、前記クライアントと前記仮想閉域網によって接続され、前記ストレージとの間の接続に使用されるプロトコルと前記仮想閉域網との間の接続に使用されるプロトコルとを変換する変換装置とで構成されるストレージシステムに用いられるストレージアクセス方法であって、前記変換装置は、前記クライアントからの前記仮想閉域網を経由したアクセス要求を受信すると、前記クライアントに割り当てられた仮想閉域網の識別情報と、該仮想閉域網に対応する前記ストレージの前記論理ボリューム内のアクセス範囲とが対応付けられたマッピング情報を参照し、前記アクセス要求に含まれる仮想閉域網の識別情報が前記マッピング情報の仮想閉域網の識別情報と一致し、前記アクセス要求に含まれるアクセス範囲が前記マッピング情報のアクセス範囲内にあった場合に、前記変換装置に接続されている前記ストレージにデータを書き込み、前記ストレージから書込終了の応答を受信すると、前記クライアントへ書込終了の応答を返信して、前記クライアントからのデータの書込処理を終了することを特徴とする。

【００１５】

【発明の作用と効果】

上記の課題を解決するために、本発明では、ストレージ及び前記ストレージを使用し、仮想閉域網に接続されたクライアントによって構成されるストレージシステムであって、前記ストレージに設定された論理ボリュームによって前記ストレージを管理する管理装置と、前記ストレージに対応するプロトコルと前記仮想閉域網で使用されるプロトコルとを変換する変換装置と、前記クライアントに割り当てられた仮想閉域網と、該仮想閉域網に対応する前記ストレージのアクセス範囲とを記憶したマッピング手段とを備えたので、不正アクセスの防止とボリューム管理のスケーラビリティを同時に実現する。

【００１６】

すなわち、クライアントがネットワーク（ＬＡＮ／ＭＡＮ／ＷＡＮ）を介したストレージへのアクセスを行うときに、クライアントが使用している仮想閉域網（ＶＰＮ）を識別して、ストレージの論理ボリューム内のアドレスへのアクセス範囲を制限する。これによって、不正アクセスや盗聴を防止することができ、かつ論理ボリューム内を分割して複数のクライアントに割り当てることでボリューム管理のスケーラビリティを向上することができる。

【００１７】

さらに、変換装置に仮想閉域網とストレージのアクセス範囲とのマッピング（変換テーブル４０、４９）を設定することにより、仮想閉域網は変換装置とストレージへの正当なアクセス権を持つクライアントとの間にしか設定されないため、仮想閉域網を識別することでクライアントを識別することが可能になり、不正アクセスを防止することができる。

【００１８】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施例について説明する。

【００１９】

図１に、本発明の第１の実施の形態のストレージシステムの構成を示す。図１に示す第１の実施の形態は、後述する他の実施の形態と異なり、内部ネットワークを前提としたネットワークに適用されるものである。図１において、２１及び２２はクライアント、２３は管理装置、２４及び２５は変換装置、２６及び２７はストレージ、５０はネットワークを示す。

【００２０】

変換装置２４には、クライアント２１及び２２、ストレージ２６、変換装置２５が接続されている。変換装置２４とクライアント２１、２２及び変換装置２５とは、ＥｔｈｅｒｎｅｔやＡＴＭ、ＩＰ等で構成されるネットワークプロトコルで接続される。変換装置２４

からストレージ２６へのアクセス要求にはｉＳＣＳＩが使用される。変換装置２４とストレージ２６とはＦＣプロトコルで接続され、ストレージへのアクセス要求にＳＣＳＩが使用される。

【００２１】

変換装置２５には、変換装置２４、管理装置２３、ストレージ２７が接続されている。変換装置２５と管理装置２３とはＥｔｈｅｒｎｅｔやＡＴＭ、ＩＰ等で構成されるネットワークプロトコルで接続され、変換装置２５とストレージ２７とはＦＣプロトコルで接続されている。

【００２２】

クライアント２１と変換装置２４との間、クライアント２２と変換装置２４との間及び変換装置２４と変換装置２５との間はＶＰＮが設定されている。

【００２３】

管理装置２３は、変換装置２４及び２５、ストレージ２６及び２７、クライアント２１及び２２を管理している。また管理装置２３は予めクライアント２１にストレージ２６及び２７の仮想ボリュームを割り当て、クライアント２１の認証後にＶＰＮ－ＩＤを持つＶＰＮを設定し、設定したＶＰＮの情報も管理する。

【００２４】

クライアント２１及び２２には、予め管理装置２３のＩＰアドレスが設定されているか、管理装置２３のＩＰアドレスを知る手段が設けられている。ＩＰアドレスを知る手段として、ディレクトリサービスやＷｅｂサービス、ＵＤＤＩ（Universal Description, Discovery and Integration）、ＤＮＳ（Domain Name System）を使用する。

【００２５】

ＵＤＤＩは、ＵＤＤＩプロジェクトが開発した仕様で、ＡＲＩＢＡ，Ｉｎｃ．とＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮとＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮとが著作権を持つ「UDDI Technical White Paper」に記載されている。ＤＮＳは、ＩＥＴＦ発行の「DOMAIN NAMES - CONCEPTS AND FACILITIES」（ＲＦＣ１０３４），「DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION」（ＲＦＣ１０３５）に記載されている。

【００２６】

図２は、クライアントが仮想ボリュームを利用するための利用手続きのシーケンス図を示す。

【００２７】

クライアント２１は、ユーザＩＤ、パスワード、クライアント情報３４を含むクライアント認証情報３３を、変換装置２４及び２５を経由して管理装置２３に送信する（処理２０１）。

【００２８】

クライアント情報３４は、ＭＡＣ（Media Access Control）アドレス、ＶＬＡＮ（Virtual LAN）タグ、ＩＰアドレス、ＴＣＰ（Transmission Control Protocol）／ＵＤＰ（User Datagram Protocol）ポート番号、Ｄｉｆｆｓｅｒｖ（Differentiated Services）で定義されているＤＳＣＰ（Diffserv Code-Point）、ＩＰｖ６ヘッダにあるフローラベル等、ＶＰＮを通過するアプリケーションやトラフィックを識別することが可能な情報である。

【００２９】

ＶＬＡＮ及びＶＬＡＮタグは、ＩＥＥＥ（The Institute of Electrical and Electronics Engineers,Inc.）発行の「IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks」（ISBN 0-7381-1538-X SS94709）に、ＤｉｆｆｓｅｒｖはＩＥＦＴ発行の「An Architecture for Differentiated Services」（ＲＦＣ２４７５）、ＤＳＣＰはＩＥＴＦ発行の「Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers」（ＲＦＣ２４７４）に規定されている。

【００３０】
処理１０１はクライアント認証処理を示す。管理装置２３はクライアント２１から受信したクライアント認証情報３３に基づいて、クライアント２１に仮想ボリュームが割り当てられているかどうかを認証する。
【００３１】
管理装置２３が管理する情報を、図３、図４、図５、図６、図７に示す。
【００３２】
図３のクライアント情報テーブル３２１は管理装置２３が管理するクライアント情報の内容を示す。Ｃｌｉｅｎｔ－ＩＤ３０４はクライアントの名前、Ａｕｔｈ３０１は認証情報、ＶＰＮ－ＩＤ３０２は接続するＶＰＮの名前、Ｖｏｌ－ＩＤ３０９は仮想ボリュームの名前を示す。図４の変換装置情報テーブル３２２は管理装置２３が管理する変換装置の内容を示す。ＴＳ－ＩＤ３１２は変換装置の名前、Ａｄｄｒｅｓｓは仮想ボリュームのアドレス、ＳＴ－ＩＤ３１３はストレージの名前、Ｖｏｌ－ＩＤ３１０は仮想ボリュームの名前を示す。図５の仮想ボリューム情報テーブル３２３は管理装置２３が管理する仮想ボリュームの内容を示す。Ｒａｎｇｅ３１８は仮想ボリュームの仮想アドレスのアドレス範囲を示す。図６のストレージ情報テーブル３２４は管理装置２３が管理するストレージ情報の内容を示す。仮想ボリューム割り当て３１５は仮想ボリュームがどのアドレスのどの範囲かを示す。図７のＶＰＮ設定情報テーブル３２５は管理装置２３が管理するＶＰＮ設定情報の内容を示す。利用クライアント情報３０３は、Ｃｌｉｅｎｔ－ＩＤ３０４とＩｎｆｏｒｍａｔｉｏｎ３０５とから構成され、それぞれクライアント名とクライアント情報とが設定される。
【００３３】
図２において、管理装置２３はクライアント２１の認証にクライアント情報テーブル３２１（図３参照）を使用する。クライアント２１からのアクセスがあったとき、管理装置２３はクライアント情報テーブル３２１を参照し、Ｃｌｉｅｎｔ－ＩＤ３０４にクライアント２１の値を持つエントリ３２６の中にあるＡｕｔｈ３０１と認証情報３３とを比較する。管理装置２３は、クライアント２１の認証に成功した場合は、クライアント情報テーブル３２１に基づいてクライアント２１用のＶＰＮ－ＩＤ３１を決定し、認証に失敗した場合はアクセスを拒否する。
【００３４】
クライアント２１の認証に成功すると、管理装置２３はＶＰＮ設定情報テーブル３２５（図７参照）に新しいエントリ３０８を作成する。エントリ３０８のＶＰＮ－ＩＤ３０２は管理装置２３がクライアント２１の認証に成功したときに決定したＶＰＮ－ＩＤ３１を設定し、利用クライアント情報３０３は認証処理１０１のときに得たクライアント２１の情報を設定する。利用クライアント情報３０３は、Ｃｌｉｅｎｔ－ＩＤ３０４とＩｎｆｏｒｍａｔｉｏｎ３０５とから構成され、それぞれクライアント２１とクライアント情報３４とが設定される。
【００３５】
ＶＰＮ設定情報テーブル３２５（図７参照）にあるエントリ３０８のＴＳ－ＩＤ３０６はオリジナル側に設定された変換装置の識別子を示し、ＴＳ－ＩＤ３０７はバックアップ側に設定された変換装置の識別子を示す。この識別子は管理装置２３がクライアントのＩＰアドレスや変換装置にアクセスするために必要な情報である。
【００３６】
ＴＳ－ＩＤ３０６及び３０７の値を設定するには、まず、クライアント２１が利用できる仮想ボリュームを知る必要がある。仮想ボリュームは、クライアント情報テーブル３２１（図３参照）のエントリ３２６の中にあるＶｏｌ－ＩＤ３０９の値として設定されている仮想ボリューム１６から得られる。次に、ストレージが接続されている変換装置の識別情報を得る必要がある。これは、仮想ボリュームは単一又は複数の論理ボリュームから構成されているので、仮想ボリュームを構成する論理ボリュームを持つストレージが存在するが、ストレージ自体の情報はエントリ３０８には必要ないためである。そこで管理装置２

３は、仮想ボリューム情報テーブル３２３（図５参照）のＶｏｌ－ＩＤ３１０から仮想ボリューム１６を持つエントリを検索し、Ｖｏｌ－ＩＤ３１０に仮想ボリューム１６の値を持つエントリ３２７のＴＳ－ＩＤ３１１の値、変換装置２４及び２５を得る。この変換装置２４及び２５を、ＶＰＮ設定情報テーブル３２５（図７）のエントリ３０８のＴＳ－ＩＤ３０６及び３０７に設定して、エントリ３０８は完成する。

【００３７】

図８に、クライアント２１に割り当てられる仮想ボリュームと実際のセキュアストレージシステムとの関係図を示す。

【００３８】

仮想ボリューム１６は、ストレージ２６内の論理ボリューム１３とバックアップ用のストレージ２７内の論理ボリューム１５とから構成される。クライアント２１が仮想ボリューム１６の利用を開始すると、管理装置２３はＶＰＮ－ＩＤ３１を割り当て、変換装置２４をオリジナル側に、変換装置２５をバックアップ側に設定し、クライアント２１にＶＰＮ－ＩＤ３１と変換装置２４の識別情報とを送信する。この識別情報によって、クライアント２１が仮想ボリューム１６にアクセス要求を送信すると変換装置２４が実際のストレージ２６の論理ボリューム１３へのアクセス要求に変換し、クライアント２１がストレージ２６にアクセスできる。

【００３９】

変換装置２４及び２５は、クライアント２１が仮想ボリュームにアクセスするときのアクセス制限、プロトコル変換、実際のストレージ２６及び２７に割り当てられている論理アドレスへのアドレス変換、等を行うための変換テーブル４０及び４９（図９、図１０参照）を持つ。

【００４０】

図９にこの変換テーブル４０の例を示す。ＶＰＮ識別子４１はクライアントが変換装置にアクセスするときのＶＰＮの識別子、アドレス範囲４２はクライアントに割り当てられた仮想ボリューム内でのデータの仮想アドレスの範囲、ストレージ識別情報４３はクライアントに割り当てられた仮想ボリュームを構成する論理ボリュームを持つストレージの識別情報、オフセット４４はストレージ識別情報４３に示されるストレージの論理アドレスを仮想アドレスから生成するためのオフセットアドレス、バックアップ変換装置４５は管理装置２３がクライアントに対してバックアップ用に設定した変換装置の識別情報を示し、変換テーブル４０にはこれらの情報の関係が規定されている。

【００４１】

ストレージ識別情報４３はＦＣポートを設定する。オフセットアドレス４４は、ＬＵＮ（Logical Unit Number）やＬＢＡ（Logical Block Address）となる。

【００４２】

図９には、ＶＰＮ識別子４１が同じでアドレス範囲４２が異なる場合の一例であるエントリ４６及び４７が示されている。エントリ４６及び４７は一つの仮想ボリュームを異なるストレージを割り当てることにより、仮想ボリューム１６を複数の論理ボリュームで構成することが可能である場合を示している。

【００４３】

エントリ４８はアドレス範囲４２とバックアップ変換装置４５の指定がない場合の一例を示している。アドレス範囲４２の指定がない場合はＶＰＮ識別子４１のみからストレージ識別情報４３とオフセットアドレス４４が決定する。バックアップ４５の指定がないことで、この変換テーブルを持つ変換装置がエントリ４８のＶＰＮ識別子４１に割り当てられている仮想ボリュームのバックアップ側の変換装置に指定されていることを示している。

【００４４】

管理装置２３は変換装置２４に、（１）ＶＰＮ識別子４１にＶＰＮ－ＩＤ３１、（２）アドレス範囲４２にクライアント２１がアクセスする仮想ボリュームの仮想アドレスのアドレス範囲ＲＡＮＧＥ１、（３）ストレージ識別情報４３にストレージ２６の識別情報、（４）オフセット４４にストレージ２６内の論理アドレスを生成するためのオフセットアド

レスＯＦＦＳＥＴ１、（５）バックアップ変換装置４５にバックアップ先の変換装置である変換装置２５の識別情報、の５つの項目からなる変換テーブルのエントリ５８と、クライアント２１のクライアント情報３４とを送信する（図２の処理２０２）。

【００４５】

同様に、管理装置２３は変換装置２５にも、（１）ＶＰＮ識別子４１にＶＰＮ－ＩＤ３１、（２）アドレス範囲４２にアドレス範囲ＲＡＮＧＥ１、（３）ストレージ識別情報４３にはストレージ２７、（４）オフセット４４にはＯＦＦＳＥＴ２、（５）バックアップ変換装置４５には変換装置２５がバックアップ側なので値は無し、の５つの項目からなる変換テーブルのエントリ５９（図１０）と、クライアント２１のクライアント情報３４とを送信する（図２の処理２０３）。

【００４６】

管理装置２３が変換装置２４の変換テーブル４０のエントリ５８を作成する手順は次のようになる。

【００４７】

管理装置２３は、ＶＰＮ－ＩＤ３１、クライアント２１、仮想ボリューム１６、変換装置２４及び２５、の値はエントリ３０８作成時に得ているが、仮想ボリュームが変換装置２４のどのストレージのどのアドレス範囲なのかはエントリ３０８作成時には検索されていないため得ていない。そこで、エントリ３０８のＴＳ－ＩＤ３０６の値である変換装置２４を変換装置情報テーブル３２２（図４）のＴＳ－ＩＤ３１２から検索し、変換装置２４を持つエントリ３２８を発見する。この検索は仮想ボリューム１６を持つストレージを発見することを目的としているので、エントリ３２８の中のＳＴ－ＩＤ３１３の値全てをストレージ情報テーブル３２４（図６）のＳＴ－ＩＤ３１４から検索し、該当するエントリの中の仮想ボリューム割り当て、３１５のＶｏｌ－ＩＤ３１６に仮想ボリューム１６が記録されているエントリ３１９を発見する。

【００４８】

一連の検索により、エントリ３１９（図６）の仮想ボリューム３１５のＯｆｆｓｅｔ３１７をエントリ５８（図９）のオフセット４４に、仮想ボリューム３１５のＲａｎｇｅ３１８をエントリ５８のアドレス範囲４２に設定し、該当したエントリ３１９のＳＴ－ＩＤ３１４をエントリ５８のストレージ識別情報４３に設定する。最後に、ＶＰＮ－ＩＤ３１をエントリ５８のＶＰＮ識別子４１に設定し、変換装置２５をエントリ５８のバックアップ変換装置４５に設定することでエントリ５８は作成される。同様の手順でエントリ５９も作成される。

【００４９】

図１１には、アクセス要求の仮想アドレスを論理アドレスに変換して、クライアント２１が変換装置２４を経由してストレージ２６とアクセスする概念図を示す。

【００５０】

図１１において、８１はネットワークプロトコルのヘッダの一例、８２はＶＰＮのヘッダの一例、８３はｉＳＣＳＩによるアクセス要求の一例、８４はＳＣＳＩによるアクセス要求の一例、８５はＦＣプロトコルのヘッダの一例を示す。クライアント２１は仮想ボリューム１６へデータ３５を書き込むため、アクセス要求８３の書き込み開始アドレス８７は仮想アドレスとなっている。実際には論理ボリューム１３にデータ３５を書き込むため、変換装置２４で仮想アドレス８７から論理アドレス８９へ変換する必要がある。

【００５１】

変換装置２４は、クライアント２１からのアクセス要求を受信すると、ＶＰＮのヘッダにあるＶＰＮ識別子８６を参照し、ＶＰＮ－ＩＤ３１を変換テーブル４０で照合し、アクセス要求８３の仮想アドレス８７をオフセットアドレス８８と仮想論理変換処理７１で論理アドレス８９に変換する。次に、変換装置２４は変換テーブル４０のエントリ５８のストレージ識別情報４３に設定されているストレージ２６を送信先９０に設定し、ＦＣプロトコルを使用してアクセス要求８４を送信する。

【００５２】

図１２に仮想論理変換処理を、図１３に論理仮想変換処理を示す。図１２は仮想アドレスを論理アドレスに変換する処理で、仮想アドレスとオフセットアドレス４４とを引数に取る関数７３によって論理アドレスに変換される。関数７３は仮想アドレスとオフセットアドレス４４とによって加算や論理和を行うことで論理アドレスを生成する関数である。図１３は論理アドレスを仮想アドレスに変換する処理で、論理アドレスとオフセットアドレス４４とを引数に取る関数７４によって仮想アドレスに変換される。関数７４は論理アドレスとオフセットアドレス４４とによって減算や論理積を行うことで仮想アドレスを生成する関数である。

【００５３】

図２において、処理１０２はＶＰＮ設定処理を示している。管理装置２３は、変換装置２４及び２５の間にＶＰＮ－ＩＤ３１によるＶＰＮ５２を設定し、変換装置２４とクライアント２１との間にもＶＰＮ－ＩＤ３１によるＶＰＮ５１を設定する。

【００５４】

処理１０３は変換装置２４への変換テーブルのエントリ設定処理を示している。管理装置２３は、変換装置２４が持つ変換テーブル４０（図９）に、変換テーブルのエントリ５８を設定する。処理１０３と同様に、処理１０４は変換装置２５への変換テーブルのエントリ設定処理を示し、管理装置２３は、変換装置２５にも管理装置２４に設定したエントリ５８と同じく、変換テーブルのエントリ５９を設定する。

【００５５】

管理装置２３は変換装置２４及び２５から処理１０２、処理１０３、処理１０４、処理１０６の結果を受信し（処理２０４）、処理結果が成功の場合、管理装置２３は認証応答を変換装置２５及び２４と経由してクライアント２１に送信する（処理２０５）。処理１０２、処理１０３、処理１０４又は処理１０６のいずれかに失敗した場合は、ＶＰＮ５１の設定と変換テーブルのエントリ５８及び５９の設定を解除し、クライアント２１のアクセスを拒否する。認証に成功した場合、クライアント２１は管理装置２３からＶＰＮ－ＩＤ３１と変換装置２４の識別情報を受信する（処理２０５）。

【００５６】

クライアント２１は、ＶＰＮ－ＩＤ３１によるＶＰＮ５１の設定処理１０７を行い変換装置２４へアクセスして、仮想ボリュームをクライアント２１で利用するためのマウント処理を行う（処理２０６）。処理１０５は仮想ボリュームのマウント処理を示す。変換装置２４はＶＰＮ－ＩＤ３１により変換テーブルのエントリ５８からクライアント２１用の仮想ボリュームに該当するストレージを２６だと認識し、変換装置２４がストレージ２６のマウント処理を行う。クライアント２１は、変換装置２４からの応答を受信し（処理２０７）、仮想ボリュームをマウントして利用を開始する。

【００５７】

図１４にクライアント２１が仮想ボリューム１６にデータ３５を書き込むときの書き込み処理のシーケンス図を示す。

【００５８】

クライアント２１はＶＰＮ－ＩＤ３１で設定されたＶＰＮ５１を経由して、変換装置２４へ書き込み命令を含むアクセス要求を送信する（処理２１１）。変換装置２４は、変換テーブル４０（図９）のＶＰＮ－ＩＤ４１にＶＰＮ－ＩＤ３１を持つエントリがあるかどうかを照合するアクセス受信処理１１１を行い、変換テーブル４０に設定されているエントリ５８を参照し、変換装置２５へのバックアップ処理１１２を行う。処理１１２の後、変換装置２４は変換装置２５へアクセス要求を送信し（処理２１２）、ストレージ２６にデータ３５の書き込みを行う処理１１３を行う。

【００５９】

変換装置２４はストレージ２６から書き込み終了の応答を受信するとストレージ応答処理１１４を行い、ストレージからの応答をクライアント２１へ返信する（処理２１３）。変換装置２５は、変換装置２４からのアクセス要求を受信すると（処理２１２）、変換装置２４の処理と同じく変換テーブル４９によるアクセス受信処理１１５を行い、ＶＰＮ－Ｉ

Ｄ３１が変換テーブル４９のエントリ５９のＶＰＮ識別子４１と一致すると、ストレージ２７へデータ３５の書き込みを行う処理１１７を行う。変換装置２５は、ストレージ２７からの応答を受信すると変換装置２４に書き込み終了の応答を返信する（処理２１４）。変換装置２４は変換装置２５からの応答を受信するとバックアップ応答処理１１６を行い、クライアント２１からの書き込み処理を完了する。

【００６０】

図１４の処理１１１の詳細なフローチャートを図１５に示す。図１５は、変換装置がアクセス要求を受信したときの処理を示している。

【００６１】

処理１２１は、変換装置がクライアントや変換装置からのアクセス要求を受信したときの処理である。処理１２２はアクセス要求を配送したＶＰＮのＶＰＮ－ＩＤが変換テーブル４０又は４９（図９、図１０）の中のＶＰＮ識別子４１にあるかどうかを照合する処理である。変換テーブルのＶＰＮ識別子４１にＶＰＮ－ＩＤが存在すれば次の処理１２３に移行する。一致しなければ処理１２６に移行し、アクセス要求を拒否する。図１４の場合、変換装置２４の変換テーブル４０の中にはエントリ５８が存在するためＶＰＮ５１のＶＰＮ－ＩＤ３１と一致するので、処理１２３に移る。処理１２３は、ＶＰＮ識別子４１から該当するエントリを抜き出し参照できるようにする。

【００６２】

処理１２４は、アクセス要求の命令の種類を判別する。アクセスが「書き込み」の場合は処理１２５に移行する。アクセスが「読み込み」の場合は処理１２８に移行する。アクセスが「書き込み」、「読み込み」以外の場合は、処理１２７に移行する。図１４の場合、アクセス要求は「書き込み」命令であるため処理１２５へ分岐する。

【００６３】

処理１２５は、アクセス要求のアドレス部分と処理１２３で参照できるようにしたエントリのアドレス範囲を照合するアクセス要求のアドレスが範囲内にあればバックアップ処理１１２に移行し、範囲外であればアクセス拒否の処理１２６に移行しクライアント２１のアクセスを拒否する。処理１２４でアクセス要求が読込み命令の場合は処理１２８にて書き込み処理と同じくアドレス範囲の照合を行う。アドレスが範囲内であればデータ読込み処理１７２に移行し、範囲外であればアクセス拒否の処理１２６へ移行する。処理１２４でのアクセス要求の命令が「読み込み」、「書き込み」のいずれでもない場合は、アクセス要求に依存した処理１２７を実行する。

【００６４】

図１４のバックアップ処理１１２の詳細なフローチャートを図１６に示す。図１６は、バックアップ側変換装置への処理を示している。

【００６５】

処理１３１は図１５の処理１２３で参照できるようにしたエントリのバックアップ４５が設定されているか否かの判断処理を示す。設定されている場合は処理１５０に移行し、設定がされていない場合はデータ書き込み処理１１３に移行する。図１４の場合、エントリ５８（図９）のバックアップ４５には変換装置２５と設定されているので、変換装置２４はバックアップ処理を行ったときに作成されるログ３６及び３７（図１７参照）を検索する処理１５０を行う。このときオリジナル側の変換装置は、バックアップ側の変換装置にアクセス要求を送信する時に二重に送信することを防ぐために、図１７に示す書き込みログテーブル３９を持っている。

【００６６】

書き込みログテーブル３９は、オリジナル側変換装置とバックアップ側変換装置とのデータ書込みの同期を取ることが目的である。ログのエントリは、アクセス要求３３０、バックアップ変換装置４５、ＶＰＮ識別子４１、ストレージ識別情報４３、データの開始アドレス３３４、から構成される。ログ３６は、オリジナル側変換装置に接続されているストレージに書き込みを開始したときのログで、ログ３７は、オリジナル側変換装置に接続されているストレージへの書き込みを終了したときのログである。

【００６７】
処理１５０は、対象となるログを検索する。ログが見つかればデータ書き込み処理１１３へ移り、見つからなければ処理１５１へ移る。処理１５１は、アクセス要求、バックアップ変換装置４５、ＶＰＮ識別子４１、を基にログ３６を作成する処理である。図１４の場合、クライアント２１からの書き込み命令と変換装置２５とＶＰＮ－ＩＤ３１とを基にログを作成する。処理１５２は、バックアップ変換装置４５に設定されている変換装置にＶＰＮ識別子４１を持つＶＰＮを経由してアクセス要求を送信する処理である。図１４の場合、ＶＰＮ５１を経由して変換装置２５にクライアント２１のアクセス要求が送信される。

【００６８】
図１４のデータ書込処理１１３の詳細なフローチャートを図１８に示す。図１８は変換装置に接続されているストレージへの書き込み処理を示す。

【００６９】
処理１３３は、図１５で参照できるようにしたエントリのオフセット４４が設定されているか否かの判断処理である。設定されていれば処理７１に移行し、設定がされていなければ処理１３４に移行する。図１４の場合、エントリ５８（図９）のオフセット４４にはＯＦＦＳＥＴ１が設定されているため、変換装置２４は仮想論理変換処理７１を行う。処理１３４は、処理７１の後、参照できるようにしたエントリのストレージ識別情報４３にアクセス要求を送信する。図１４の場合、エントリ５８のストレージ識別情報４３にはストレージ２６が設定されているので、変換装置２４はストレージ２６にアクセス要求を送信する。

【００７０】
図１４のストレージ応答処理１１４の詳細を図１９に示す。図１９は、変換装置２４がストレージ２６へ書き込み命令を送信した後ストレージ２６からの応答を受信したときの処理を示す。

【００７１】
処理１４１は、データ書込み処理の後変換装置がストレージからの応答を待つ。ストレージからの応答を受信すると処理１４２へ移行する。処理１４２は図１５において参照できるようにしたエントリのバックアップ４５が設定されているか否かの判断処理である。設定されていると処理１５３に移行する。設定がされていないと処理１４４に移行する。図１４の場合、エントリ５８のバックアップ４５には変換装置２５と設定されているため、変換装置２４は処理１５３を行う。

【００７２】
処理１５３は、ストレージへの書き込み処理時のアクセス要求から作成されるログ３６が書き込みログテーブル３９（図１７）に存在するか否かを検索する。ログ３６が存在しない場合はバックアップ側の変換装置での書き込み処理が既に完了していると判断し、処理１４４に移行する。ログ３６が残っている場合は、ログ３６に実際に書き込んだストレージと論理アドレスの情報を追加する処理１５４に移行する。図１４の場合、ログ３６にストレージ２６と論理アドレス８９を追記し、状態３３１を「書き込み後」と変更する。

【００７３】
処理１５４は、ログ３６をログ３７に変更する。処理１４４は、図１５において参照できるようにしたエントリのオフセット４４が設定されているか否かの判断処理である。設定されていれば処理７２に移行し、設定がされていなければ処理１４５に移行する。図１４の場合、エントリ５８のオフセット４４にはＯＦＦＳＥＴ１が設定されているため、変換装置２４は論理仮想変換処理７２を行う。

【００７４】
処理１４５は、アクセス要求を送信してきたアクセス元へストレージからの応答を送信する。図１４の場合、クライアント２１がアクセス元なのでクライアント２１にストレージ２６からの応答をＶＰＮ５１経由で送信する。クライアント２１は変換装置２４から応答を受信し（図５の処理２１３）、書き込み処理を完了する。

【００７５】
図１４のバックアップ応答処理１１６の詳細なフローチャートを図２０に示す。図２０は、バックアップ先の変換装置からの応答処理である。
【００７６】
処理１６１はバックアップ先の変換装置からの応答を受信する処理で、応答を受信すると処理１６２へ移行する。処理１６２は、アクセス要求とバックアップ先の変換装置４５とＶＰＮ識別子４１とから該当するログ３６及び３７（図１７参照）を検索する。ログが存在しない場合はバックアップ先の変換装置にアクセス要求を送信したことがないことを示し処理１６３に移行しアクセスを拒否する。ログが見つかった場合は処理１６４に移行する。
【００７７】
処理１６４はアクセス要求の処理内容を判断する。処理内容が書き込み終了なら処理１６５に移行し該当するログの消去を行いバックアップ応答処理１１６を終了する。
【００７８】
処理内容が再送なら処理１６６に移行する。処理１６６は、ログの種類の判別処理を行う。ログの種類が実際に書き込んだストレージの情報などが追加された書込終了を示す「書込後」状態のログ（例えば、ログ３７）の場合は処理１６７へ移行し、書き込みが終了していないことを示す「書込前」状態のログ（例えば、ログ３６）の場合は処理１６８に移行する。処理１６７は、ログ３７の情報からアクセス要求を生成しバックアップ先の変換装置へ再送する。
【００７９】
一方、処理１６８は、該当するアクセス要求を実際のストレージに書き込むために仮想アドレスから論理アドレスに変換したアクセス要求を持つプロセスが、変換装置内で稼動している状態にある。そのため、該当するログ３６を消去して、保持しているアクセス要求のヘッダの論理アドレスを仮想アドレスに変換してから該当するプロセスにバックアップ開始処理１３２を再度行わせる。
【００８０】
図１４の処理２１４の場合、ストレージ２６への書き込みが完了した時点で、変換装置２５からの応答が送信される。そのため、書き込みが完了したときのログ３７が生成された後にバックアップ応答処理が処理され、バックアップ応答処理１１６ではログ３７が消去されることになる。書き込みログテーブル３９によるバックアップ処理の管理により、バックアップ先の変換装置から書き込み終了の応答があるまでログ３６又は３７は保持されデータの同期が保証される。したがって、クライアント２１へは変換装置２４での書き込み処理が終わった段階で応答を1度返信するだけでよく、変換装置２５からの応答は変換装置２４まででクライアント２１へは返信しない。また、消去対象になるログを消去せずに残しておくことも可能で、その場合は該当するログの消去時にログの状態３３１の値を「完了」とする。
【００８１】
図２１に、クライアント２１の仮想ボリューム１６からの読込み処理のシーケンス図を示す。
【００８２】
クライアント２１が仮想ボリューム１６からデータを読み込む場合、クライアント２１はＶＰＮ－ＩＤ３１で設定されたＶＰＮ５１を経由して変換装置２４へ読み込み命令を含むアクセス要求を送信する（処理２７１）。変換装置２４は、変換テーブル４０（図９）のＶＰＮ識別子４１にＶＰＮ－ＩＤ３１を持つエントリがあるか照合し（処理１１１）、設定されているエントリ５８を参照し、ストレージ２６から読み込みを行う（処理１７２）。変換装置２４は、ストレージ２６からデータ３８を含む読み込み終了の応答を受信すると、クライアント２１に応答を返信して（処理２７２）、クライアント２１からの読み込み処理を完了する。
【００８３】

図２１の処理１１１は図１５に示すアクセス受信処理であり、図２１はクライアントがデータを読み込むときの処理であるため、アクセス受信処理１１１の後、データ読込み処理１７２に移る。

【００８４】

図２２は、変換装置に接続されているストレージからのデータ読込み処理（図２１の処理１７２）の詳細なフローチャートを示す。

【００８５】

処理１３２は、図１５で参照できるようにしたエントリのオフセット４４（図９）が設定されているか否かの判断処理である。設定されていれば処理７１に移行する。設定がされていなければ処理１３３に移行する。図２１の場合、エントリ５８のオフセット４４にＯＦＦＳＥＴ１が設定されているので変換装置２４は仮想論理変換処理７１を行う。

【００８６】

処理７１を行った後、図１５において参照できるようにしたエントリのストレージ識別情報４３にアクセス要求を送信する処理１３３を行う。図２１の場合、エントリ５８のストレージ識別情報４３にはストレージ２６と設定されているので、変換装置２４はストレージ２６へアクセス要求を送信する。処理１４１は、ストレージ２６からの応答を受信する処理である。処理７２で、変換装置２４は論理仮想変換処理を行う。処理１４４は、データ３８を含むアクセス要求をクライアント２１へ返信する。

【００８７】

処理１３２でオフセットアドレス４４が設定されていない場合は、変換装置はアドレスを変換せずにアクセス要求をストレージ２６に中継する。クライアント２１の仮想ボリューム利用終了手続きは、クライアント２１からＶＰＮ－ＩＤ３１とクライアント認証情報３３を管理装置２３に送信し、管理装置２３は変換装置２４及び２５からＶＰＮ－ＩＤ３１の変換テーブルのエントリを削除して、クライアント２１用のＶＰＮ５１を解除する。

【００８８】

図２３には、クライアント２１の仮想ボリューム１６からデータの読込処理でストレージ２６に障害が発生した場合のシーケンス図を示す。

【００８９】

クライアント２１が仮想ボリューム１６からデータの読み込みを行う場合、クライアント２１はＶＰＮ５１を経由して変換装置２４へ読み込み命令を送信する（処理２７１）。変換装置２４は変換テーブル４０（図９）による照合を行い（処理１１１）、設定されているエントリ５８を参照して、ストレージ２６からデータの読み込みを行う。このとき、ストレージ２６からの応答がない又は失敗応答を受信すると、ストレージ２６に障害が発生したと判断する（処理１７３）。

【００９０】

ストレージ２６に障害が発生して読み込みが失敗した場合は、変換装置２４はアクセス要求のヘッダの論理アドレス部分を仮想アドレスに変換してから変換装置２５に送信する（処理２７３）。変換装置２５は、変換装置２４と同様に変換テーブル４０による照合を行い（処理１７４）、エントリ５９を参照してストレージ２７から読込みを行いデータ３８を受け取り（処理１７５）、変換装置２４にデータ３８を含むストレージからの応答を転送する（処理２７４）。

【００９１】

変換装置２４は、変換装置２５から受信したストレージからの応答をクライアント２１へ送信する（処理２７２）。クライアント２１の読込み処理が完了した後に、変換装置２４は管理装置２３へ障害情報を送信する（処理２７５）。

【００９２】

管理装置２３は、新しいバックアップ先や差分用の仮想ボリュームを割り当てて、クライアント２１からのデータ読み込み／書き込み命令への準備を行う（処理１７６）。差分用の仮想ボリュームが割り当てられたときは、元のストレージが復旧するまで書き込みのログ３７を残しておき、元のストレージが復旧した時点で差分用の仮想ボリュームからログ

３７を元に最新の状態に戻して同期をとる。この一連の動作によって、障害発生時でも書き込みデータの同期をとることが可能となる。

【００９３】

ＶＰＮの種類としては、ＭＰＬＳ－ＶＰＮや、ＩＰ－ＶＰＮ、ＩＰｓｅｃによるＶＰＮ、ＡＴＭをＶＰＮに使用する場合にはＳＶＣ（Switched Virtual Circuit）を想定している。ＶＰＮの設定手段としては、ＣＯＰＳ（Common Open Policy Service）等ポリシー配布による設定やオペレータの操作による設定を想定している。ＭＰＬＳはＩＥＴＦ発行の「Multiprotocol Label Switching Architecture」（ＲＦＣ３０３１）に、ＭＰＬＳ－ＶＰＮはＩＥＴＦ発行の「BGP/MPLS VPNs」（ＲＦＣ２５４７）に、ＣＯＰＳはＩＥＴＦ発行の「The COPS(Common Open Policy Service) Protocol」（ＲＦＣ２７４８）、「COPS Usage for Policy Provisioning(COPS-PR)」（ＲＦＣ３０８４）に記載されている。

【００９４】

上記のように構成された第１の実施の形態では、ＶＰＮ機能を持つクライアント又はネットワークノードと、ＳＡＮ等で構成されるストレージと、ストレージの容量やストレージに割り当てられた論理ボリュームを管理する手段を持つ管理装置と、ストレージで使用されるＳＡＮ等のプロトコルとＬＡＮ／ＭＡＮ／ＷＡＮ内で使用されるプロトコルを相互変換するプロトコル変換手段と、ＶＰＮ機能を持つ変換装置と、を備える。また、セキュリティ対策として、クライアントと変換装置との間に単一又は複数の種類によるＶＰＮを設定し、変換装置とストレージとの間にゾーニング機能によるマッピングを設定し、変換装置にＶＰＮとストレージのアクセス範囲とのマッピングを設定するマッピング手段を備える。ＶＰＮは変換装置とストレージへの正当なアクセス権を持つクライアントとの間にしか設定されないため、ＶＰＮを識別することでクライアントを識別することが可能になる。ＶＰＮの識別にはＶＰＮ－ＩＤを使用し、ストレージのアクセス範囲は論理ボリューム内のアドレスを使用する。これによって、不正アクセスの防止とボリューム管理のスケーラビリティを同時に実現することができる。

【００９５】

すなわち、クライアントと変換装置との間に設定されたＶＰＮはストレージ側には設定されないが、変換装置とストレージとの間に設定されたＳＡＮはＬＡＮ／ＭＡＮ／ＷＡＮに接続されたクライアントと直接通信することができないため、変換装置を必ず経由しなければならず、変換装置にＶＰＮ－ＩＤが設定されていないクライアントからのストレージへのアクセスは変換装置で拒否するので、変換装置からストレージ側へのセキュリティは確保される。また、ＶＰＮ－ＩＤを使用して、ＶＰＮとストレージのアクセス範囲とのマッピング手段をすることによって、ストレージへのアクセス制限だけでなくＶＰＮ－ＩＤごとにストレージのアクセス範囲が管理できるため、ＳＡＮのポート数に制限されるボリューム監視よりもクライアントへのボリューム割り当て数を増加させることが可能になる。これによって、不正アクセスや盗聴を防止することができ、かつ論理ボリューム内を分割して複数のクライアントに割り当てることでボリューム管理のスケーラビリティを向上することができる。さらに、変換装置２４をオリジナル側、変換装置２５をバックアップ側に設定し、オリジナル側のストレージ２６に障害が発生した場合には、管理装置２３によってその障害を検出し、バックアップ側のストレージ２７によって障害の起こったデータを救済することができる。

【００９６】

図２４には、本発明の第２の実施の形態のストレージシステムを示す。２１及び２２はクライアント、２３は管理装置、２４及び２５は変換装置、２６及び２７はストレージ、２８及び２９はネットワークノード、３０はネットワーク制御装置である。ネットワークノード２８、２９はルータやスイッチ等と呼ばれるものでＶＰＮの設定が可能なものとする。ネットワーク制御装置３０は変換装置２４及び２５やネットワークノード２８及び２９に対してＶＰＮの設定を行い、ＶＰＮ－ＩＤ３１を持つトラフィックに対して通信品質（ＶＰＮのトラフィック、ＱＯＳの優先設定等）の設定や冗長構成を設定する。クライアント２１及び２２にはＶＰＮを設定する手段を設ける必要はない。５０はネットワークを示

しており、該ネットワークにはクライアントからのストレージへのアクセスの障害になるトラフィックが流れており、ネットワーク制御装置３０によって、ネットワークに対して帯域幅確保などの通信品質の設定を行う。

【００９７】

変換装置２４には、変換装置２５、ストレージ２６、ネットワークノード２９が接続されている。変換装置２４と変換装置２５及びネットワークノード２６とはネットワークプロトコルによって、変換装置２４とストレージ２６とはＦＣプロトコルによって接続される。ネットワークノード２９にはネットワークノード２８、ネットワーク制御装置３０がネットワークプロトコルで接続されている。ネットワークノード２８にはクライアント２１及び２２がネットワークプロトコルで接続されている。変換装置２５には、管理装置２３とストレージ２７とが接続され、変換装置２５と管理装置２３とはネットワークプロトコルで、変換装置２５とストレージ２７とはＦＣプロトコルで接続される。

【００９８】

ネットワークノード２８及び２９の間、ネットワークノード２９と変換装置２４との間、変換装置２４及び２５の間にはネットワーク制御装置３０によって、ＶＰＮの設定が可能である。また、ネットワーク制御装置３０はネットワークノード２８にクライアント情報とＶＰＮへのマッピングとを設定することができる。

【００９９】

第２の実施の形態のストレージシステムによると、クライアント２１は、ネットワーク上にある割り当てられた仮想ボリュームを利用するための利用手続きを行うために、第１の実施の形態のストレージシステムと同様にクライアント認証情報３３を管理装置２３に送信する。管理装置２３はクライアント２１の認証に成功した場合、クライアント２１用のＶＰＮ－ＩＤ３１を決定し、第１の実施例と同じく変換装置２４及び２５に変換テーブル４０のエントリ５８及び５９とクライアント情報３４を設定し、ネットワーク制御装置３０にクライアント２１のクライアント情報３４とＶＰＮ－ＩＤ３１を送信し、クライアント２１にＶＰＮ－ＩＤ３１と変換装置２４のアドレスを送信する。

【０１００】

ネットワーク制御装置３０はＶＰＮ－ＩＤ３１によるＶＰＮ５１をネットワークノード２８及び２９、変換装置２４の間に設定し、ＶＰＮ５２を変換装置２４及び２５の間に設定し、ネットワークノード２８には、クライアント２１のクライアント情報３４によるトラフィックとクライアント２１用のＶＰＮ５１へのマッピングを設定する。以降の処理は、前記第１の実施例と同様である。

【０１０１】

第２の実施例をセキュリティ面で見た場合、クライアント２１とネットワークノード２８との間にはＶＰＮ５１は設定されない点が問題になりそうだが、ネットワークノード２８でクライアント２１を識別して他のトラフィックとは区別するため、セキュリティは確保される。

【０１０２】

第２の実施例では、帯域幅確保や通信パスの設定には、ＭＰＬＳ（Multiprotocol Label Switching）やＭＰＬＳの拡張プロトコル、ＧＭＰＬＳ（Generalized MPLS）シグナリング、ポリシールーティング、Ｄｉｆｆｓｅｒｖ、ＲＳＶＰ（Resource Reservation Protocol）、ＡＴＭ（Asynchronous Transfer Mode）のＶＰ（Virtual Path）／ＶＣ（Virtual Channel）設定を使用する。ＧＭＰＬＳシグナリングはＩＥＴＦ発行の「Generalized MPLS - Signaling Functional Description」（draft-ietf-mpls-generalized-signaling）に記載されている。

【０１０３】

ネットワーク制御装置３０と管理装置２３との間のインターフェースには既にネットワークを管理するサーバがあり任意のＶＰＮ－ＩＤによるＶＰＮの設定が可能であれば、そのサーバへの設定手段を使用する。ネットワーク制御装置３０に外部からの設定手段がない場合には、予めＶＰＮを設定しておきクライアントからの利用手続きを処理した段階でＶ

ＰＮが有効になるように変換装置に該当する変換テーブルのエントリを設定することで有効になるものとする。

【０１０４】

上記のように構成された第２の実施の形態のセキュアストレージシステムでは、前記第１の実施の形態の効果に加え、ネットワークノードにクライアントとＶＰＮのマッピングを設定することで、クライアントに対して直接ＶＰＮを設定できない場合でもストレージへのアクセスのセキュリティを確保することができる。

【０１０５】

図２５に、本発明の第３の実施の形態のストレージシステムを示す。ネットワークノード２８はスイッチに相当し、ＶＰＮの機能を持たないがＶＬＡＮの設定が可能である。ネットワークノード２９は、ルータに相当するもので、ＶＬＡＮとＶＰＮの機能を持ち、ＶＬＡＮとＶＰＮのマッピングが可能である。なお、第１又は第２の実施の形態と同一の動作をする構成には同一の符号を付して、その詳細な説明は省略する。

【０１０６】

ネットワークノード２８及び２９との間はＶＬＡＮで接続される。ネットワークノード２９と変換装置２４との間と、変換装置２４及び２５との間はＶＰＮで接続される。ネットワーク制御装置３０はネットワークノード２９、変換装置２４及び２５にＶＰＮを、ネットワークノード２８及び２９にＶＬＡＮを設定することができ、ネットワークノード２８にはクライアント情報とＶＬＡＮへのマッピングを、ネットワークノード２９にはＶＬＡＮとＶＰＮへの設定することができる。

【０１０７】

管理装置２３からクライアント２１用のＶＰＮ５１の設定要求を受信した場合は、ネットワーク制御装置３０は、変換装置２４とネットワークノード２９の間にＶＰＮ５１を設定し、変換装置２４と変換装置２５の間にＶＰＮ５２を設定し、ネットワークノード２８及び２９の間にＶＬＡＮ５３を設定する。ＶＬＡＮ５３は管理装置２３から受信したＶＰＮ－ＩＤ３１と対応させてネットワーク制御装置３０で決定、管理する。ネットワークノード２８には、クライアント２１のクライアント情報３３によるトラフィックとクライアント２１用のＶＬＡＮ５３へのマッピングを設定し、ネットワークノード２９には、クライアント２１用のＶＬＡＮ５３とクライアント２１用のＶＰＮ５１へのマッピングを設定する。その他の処理は第２の実施の形態と同様である。

【０１０８】

上記のように構成された第３の実施の形態のセキュアストレージシステムでは、前記第１の実施の形態の効果に加え、クライアントとネットワークノードとの間にＶＬＡＮを設定しても、ＶＰＮ－ＩＤを用いてＶＬＡＮとＶＰＮとのマッピングを行うことにより、ＶＬＡＮ上のクライアントからストレージへのアクセスのセキュリティを確保することができる。

【０１０９】

図２６に、本発明の第４の実施の形態のストレージシステムを示す。なお、第１～第３の実施の形態と同一の動作をする構成には同一の符号を付して、その詳細な説明は省略する。

【０１１０】

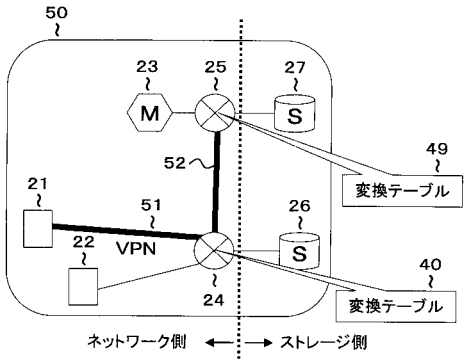
２１及び２２はクライアント、２４及び２５は変換装置、２６及び２７はストレージ、２３は管理装置、３０はネットワーク制御装置、２８はネットワークノード、７はＬＡＮやＳＡＮで構成されている内部ネットワーク、８はＭＡＮやＷＡＮなどの外部ネットワークである。変換装置２４及び２５、ネットワークノード２８にはＶＰＮの設定が可能である。内部ネットワーク７、外部ネットワーク８には各ネットワークに１つずつネットワーク制御装置３０が配置されており、ネットワーク制御装置３０は、各ネットワーク内のネットワークノード２８や変換装置２４及び２５に対して、管理装置２３から送信されたＶＰＮ－ＩＤ３１によるＶＰＮ５１及び５２の設定、解除やＶＬＡＮとＶＰＮのマッピング、クライアント情報に基づくＶＰＮ／ＶＬＡＮの設定が行えるものとする。

【０１１１】
上記のように構成された第４の実施の形態のセキュアストレージシステムでは、前記第１の実施の形態の効果に加え、ＶＬＡＮを設定したＭＡＮやＷＡＮなどの大規模なネットワーク上のクライアントからストレージへのアクセスのセキュリティを確保することができる。
【０１１２】
第１の実施の形態のストレージシステムの変形例である第５の実施の形態について説明する。第５の実施の形態のストレージシステムは、変換装置２５の変換テーブル４９のエントリ５９（図１０）内で、バックアップ変換装置４５に変換装置２４を指定したものであり、変換装置２５が変換装置２４のバックアップ装置になると共に、変換装置２４が変換装置２５のバックアップとなる。なお、第１の実施の形態と同一の動作をする構成には同一の符号を付して、その詳細な説明は省略する。
【０１１３】
変換装置２４は変換装置２５から見るとバックアップ変換装置となるため、変換装置２５もオリジナルの変換装置２４と同様に、別のクライアントのアクセスを処理して負荷を分散させることができる。管理装置２３はクライアントからの仮想ボリューム利用手続きの認証応答でクライアントのアクセスが分散されるように、もしくはアクセス速度が短くなるように、適切な変換装置の識別情報を返送することができる。
【０１１４】
上記のように構成された第５の実施の形態のセキュリティストレージシステムでは、前記第１の実施の形態の効果に加え、変換装置２４は変換装置２５をバックアップに、変換装置２５は変換装置２４をバックアップに、それぞれ設定するので、お互いへのアクセスが分散され、アクセス速度を短くすることができる。
【図面の簡単な説明】
【図１】本発明の第１の実施の形態における、ネットワーク構成図である。
【図２】本発明の第１の実施の形態における、クライアントによる仮想ボリュームの利用手続きを示すシーケンス図である。
【図３】本発明の第１の実施の形態における、管理装置が管理するクライアント情報テーブルの説明図である。
【図４】本発明の第１の実施の形態における、管理装置が管理する変換装置情報テーブルの説明図である。
【図５】本発明の第１の実施の形態における、管理装置が管理する仮想ボリューム情報テーブルの説明図である。
【図６】本発明の第１の実施の形態における、管理装置が管理するストレージ情報テーブルの説明図である。
【図７】本発明の第１の実施の形態における、管理装置が管理するＶＰＮ設定情報テーブルの説明図である。
【図８】本発明の第１の実施の形態における、仮想ボリュームと論理ボリュームとの関係の説明図である。
【図９】本発明の第１の実施の形態における、変換装置２４の変換テーブルの説明図である。
【図１０】本発明の第１の実施の形態における、変換装置２５の変換テーブルの説明図である。
【図１１】本発明の第１の実施の形態における、クライアントのアクセス要求のアドレス変換と通信プロトコル変換の説明図である。
【図１２】本発明の第１の実施の形態における、仮想アドレスから論理アドレスへのアドレス変換処理のフローチャートである。
【図１３】本発明の第１の実施の形態における、論理アドレスから仮想アドレスへのアドレス変換処理のフローチャートである。
【図１４】本発明の第１の実施の形態における、クライアントによる仮想ボリュームへの

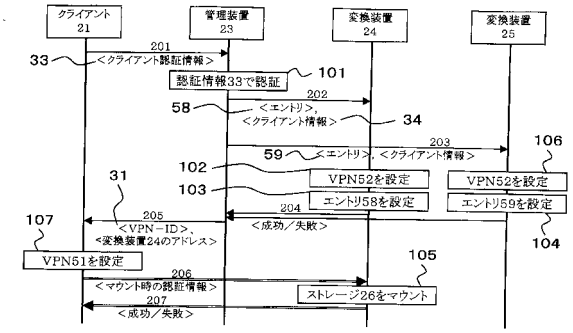
書き込み処理のシーケンス図である。
【図１５】本発明の第１の実施の形態における、変換装置によるクライアントからの仮想ボリュームへのアクセス受信処理のフローチャートである。
【図１６】本発明の第１の実施の形態における、変換装置によるバックアップ側変換装置へのバックアップ処理のフローチャートである。
【図１７】本発明の第１の実施の形態における、ログテーブルの説明図である。
【図１８】本発明の第１の実施の形態における、変換装置によるストレージへのデータ書込み処理のフローチャートである。
【図１９】本発明の第１の実施の形態における、変換装置によるストレージ応答処理のフローチャートである。
【図２０】本発明の第１の実施の形態における、変換装置によるバックアップ応答処理のフローチャートである。
【図２１】本発明の第１の実施の形態における、クライアントによる仮想ボリュームからの読込み処理のシーケンス図である。
【図２２】本発明の第１の実施の形態における、変換装置によるデータ読込み処理のフローチャートである。
【図２３】本発明の第１の実施の形態における、障害発生時の処理のシーケンス図である。
【図２４】本発明の第２の実施の形態における、ネットワーク構成図である。
【図２５】本発明の第３の実施の形態における、ネットワーク構成図である。
【図２６】本発明の第４の実施の形態における、複数のネットワークを含むネットワーク構成図である。
【図２７】従来技術のＦＣポートを用いたボリューム管理の説明図である。
【符号の説明】
７　内部ネットワーク（ＬＡＮ／ＳＡＮ）
８　外部ネットワーク（ＭＡＮ／ＷＡＮ）
１１　ストレージ
１２、１４　ＦＣポート
１３、１５　ストレージ内の論理ボリューム
１６　仮想ボリューム
２１、２２　クライアント
２４、２５　変換装置
２６、２７　ストレージ
２８、２９　ネットワークノード（ルータ、スイッチ）
３０　ネットワーク制御装置
３１　クライアント２１用ＶＰＮ－ＩＤ
３３　クライアント２１の認証情報
３４　クライアント２１の識別情報
３５　ストレージに書き込むデータ
３６　変換装置２５との同期用ログ
３７　ストレージ２６へ書き込みが完了したときの、変換装置２５との同期用ログ
３８　ストレージから読み出したデータ
３９　同期用ログを管理する書き込みログテーブル
４０　変換装置２４が持つ変換テーブル
４１　対象となるＶＰＮ－ＩＤ
４２　対象となる仮想ボリュームのアドレス範囲
４３　仮想ボリュームを構成している論理ボリュームを持つストレージ識別情報
４４　ストレージ４３の論理アドレスを仮想アドレスから生成するためのオフセットアドレス
４５　バックアップ側の変換装置の識別情報

４６　変換テーブルのエントリで、仮想アドレスのアドレス範囲によって論理ボリュームが異なる場合の例
４７　変換テーブルのエントリで、仮想アドレスのアドレス範囲によって論理ボリュームが異なる場合の例
４８　変換テーブルのエントリで、バックアップ用の変換装置の識別情報がない場合の例
４９　変換装置２５が持つ変換テーブル
５０　ネットワーク
５１　クライアント２１用のＶＰＮ
５２　ＶＰＮ－ＩＤ３１を持つ変換装置２４，２５間のＶＰＮ
５３　クライアント２１用のＶＬＡＮ
５８　実施例で変換装置２４に追加される変換テーブルのエントリ
５９　実施例で変換装置２５に追加される変換テーブルのエントリ
７３　仮想アドレスから論理アドレスに変換する関数
７４　論理アドレスから仮想アドレスに変換する関数

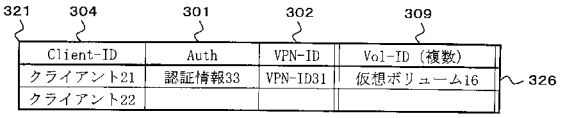
【図１】



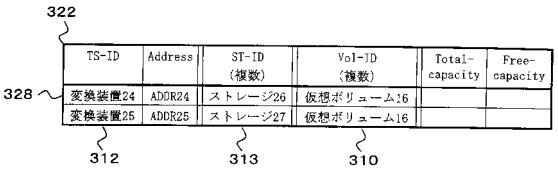
【図２】



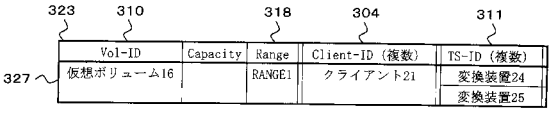
【図３】


321
304
301
302
309
Client-ID
Auth
VPN-ID
Vol-ID（複数）
クライアント21
認証情報33
VPN-ID31
仮想ボリューム16
クライアント22
326

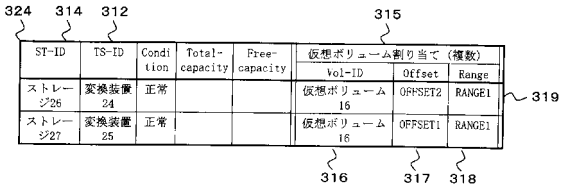
【図４】


322
TS-ID
Address
ST-ID（複数）
Vol-ID（複数）
Total-capacity
Free-capacity
328
変換装置24
ADDR24
ストレージ26
仮想ボリューム16
変換装置25
ADDR25
ストレージ27
仮想ボリューム16
312
313
310

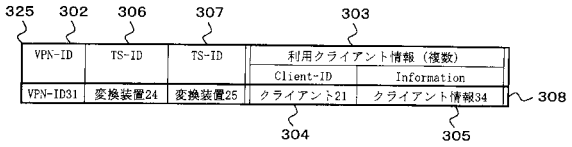
【図５】


323
310
318
304
311
Vol-ID
Capacity
Range
Client-ID（複数）
TS-ID（複数）
327
仮想ボリューム16
RANGE1
クライアント2i
変換装置24
変換装置25

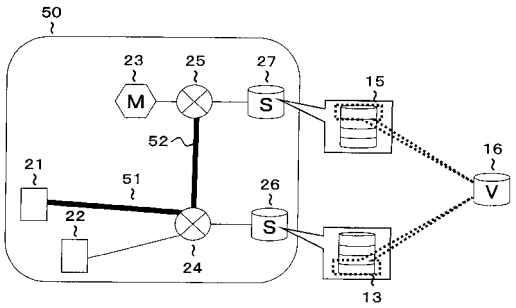
【図６】


324
314
312
315
ST-ID
TS-ID
Condition
Total-capacity
Free-capacity
仮想ボリューム割り当て（複数）
Vol-ID
Offset
Range
ストレージ26
変換装置24
正常
仮想ボリューム16
OFFSET2
RANGE1
319
ストレージ27
変換装置25
正常
仮想ボリューム16
OFFSET1
RANGE1
316
317
318

【図７】



【図８】



【図９】

40

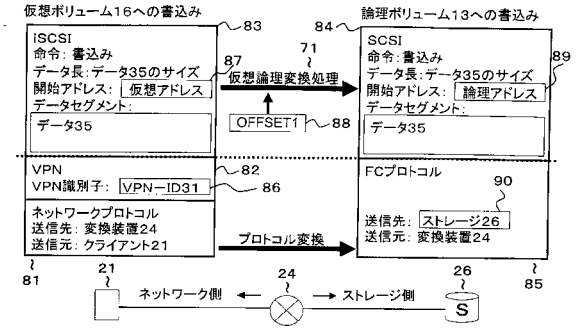
ネットワーク側情報		ストレージ側情報		バックアップ変換装置	
VPN識別子	アドレス範囲	ストレージ識別情報	オフセット		
100000-00000001	0-4000	FC-PORT1	OFFSET2	10.100.1.5	46
	4000-10000	FC-PORT2	OFFSET1	10.100.1.5	47
100000-00000065	＜なし＞	FC-PORT1	OFFSET1	＜なし＞	48
VPN-ID31	RANGE1	ストレージ26	OFFSET1	ADDR25	58
41	42	43	44	45	

【図１０】

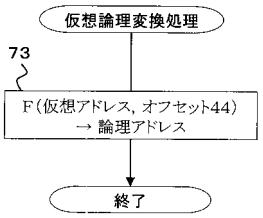
49

ネットワーク側情報		ストレージ側情報		バックアップ変換装置	
VPN識別子	アドレス範囲	ストレージ識別情報	オフセット		
100000-00000011	0-4000	FC-PORT1	OFFSET1	10.100.2.5	
100000-00001065	0-10000	FC-PORT1	OFFSET2	10.100.2.5	
VPN-ID31	RANGE1	ストレージ27	OFFSET2	＜なし＞	59
41	42	43	44	45	

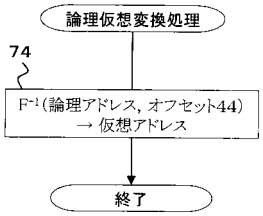
【図１１】



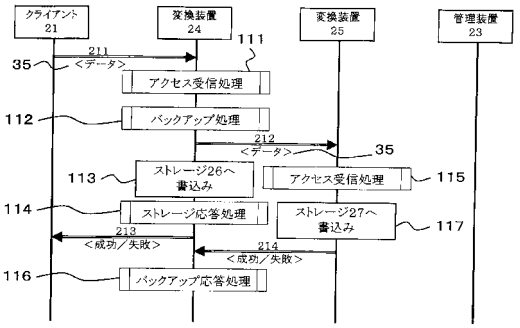
【図１２】



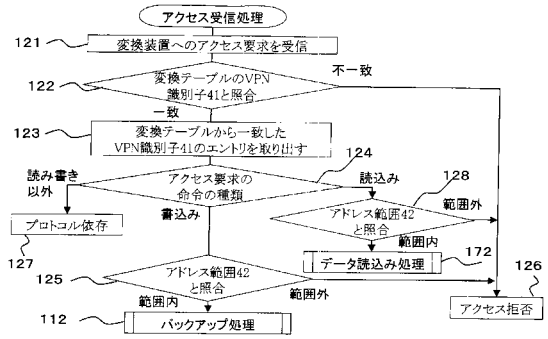
【図１３】



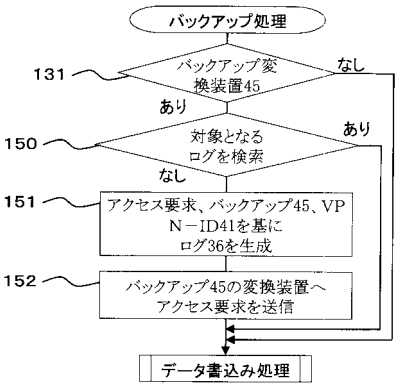
【図１４】



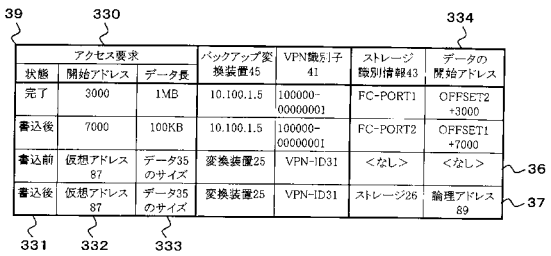
【図１５】



【図１６】



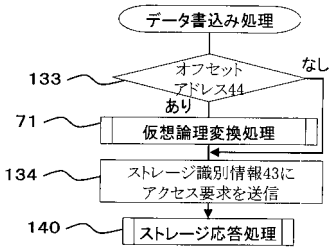
【図１７】



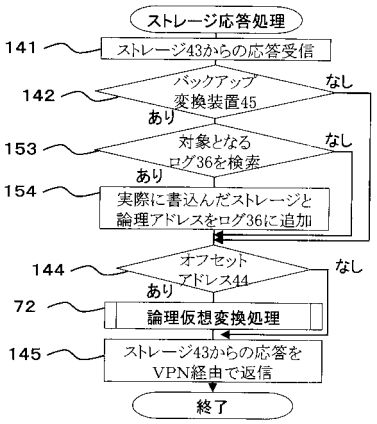
39	330					334
アクセス要求			バックアップ変換装置45	VPN識別子41	ストレージ識別情報43	データの開始アドレス
状態	開始アドレス	データ長				
完了	3000	1MB	10.100.1.5	100000-00000001	FC-PORT1	OFFSET2 +3000
書込後	7000	100KB	10.100.1.5	100000-00000001	FC-PORT2	OFFSET1 +7000
書込前	仮想アドレス87	データ35のサイズ	変換装置25	VPN-ID31	<なし>	<なし>
書込後	仮想アドレス87	データ35のサイズ	変換装置25	VPN-ID31	ストレージ26	論理アドレス89

36
37
331 332 333

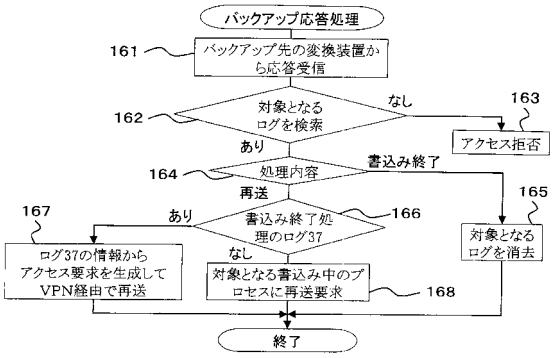
【図１８】



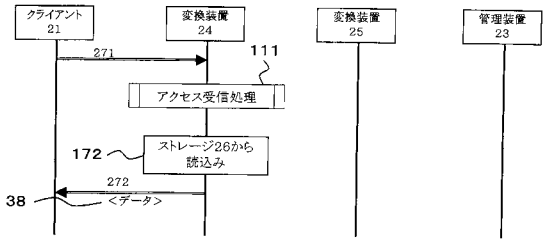
【図１９】



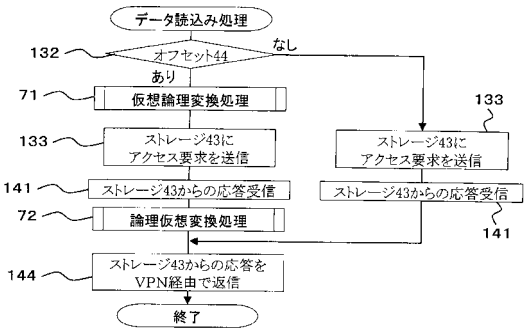
【図２０】



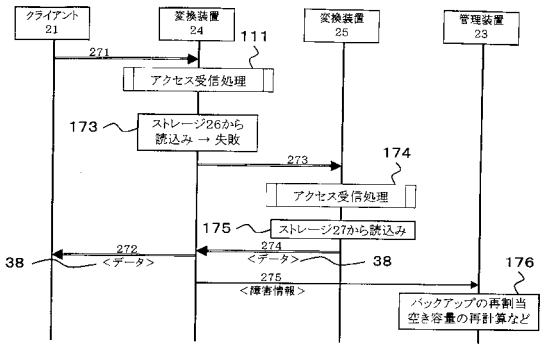
【図２１】



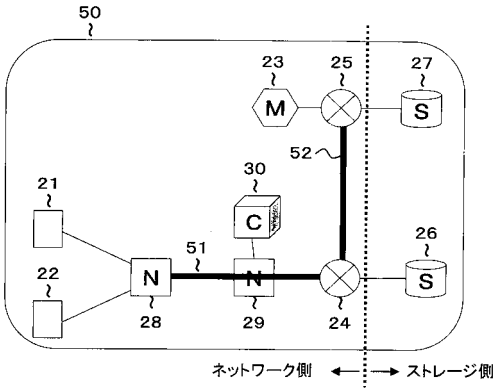
【図２２】



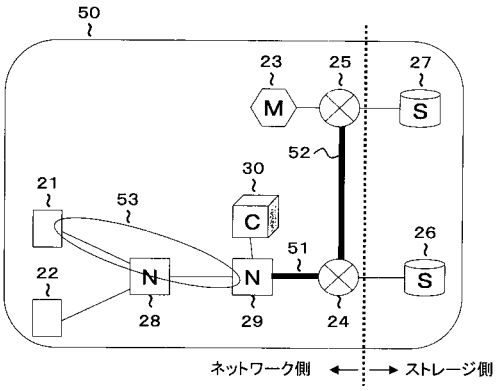
【図２３】



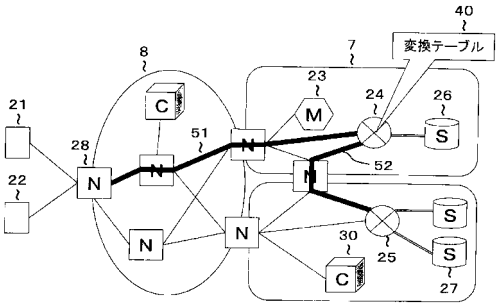
【図２４】



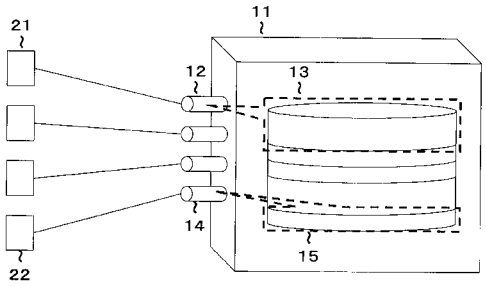
【図２５】



【図２６】



【図２７】



フロントページの続き

(51)Int.Cl. FI
G06F 12/00 545A
G06F 3/06 301K
G06F 3/06 304H

(72)発明者 宮城 盛仁
東京都国分寺市東恋ヶ窪一丁目２８０番地 株式会社日立製作所 中央研究所内
(72)発明者 赤羽 真一
東京都国分寺市東恋ヶ窪一丁目２８０番地 株式会社日立製作所 中央研究所内
(72)発明者 水谷 昌彦
東京都国分寺市東恋ヶ窪一丁目２８０番地 株式会社日立製作所 中央研究所内

審査官 小林 秀和

(56)参考文献 国際公開第０２／００３２２０（WO，Ａ１）
特開２００２－０７７２７５（ＪＰ，Ａ）
特開２００２－０１４７７７（ＪＰ，Ａ）
国際公開第０２／００３２０３（WO，Ａ１）
特開２００２－１６４９３７（ＪＰ，Ａ）
特開２００３－１２４９７６（ＪＰ，Ａ）
特開２００３－０３２２７５（ＪＰ，Ａ）
米国特許出願公開第２００２／００６９３６９（ＵＳ，Ａ１）
米国特許出願公開第２００１／００３４７５８（ＵＳ，Ａ１）
米国特許出願公開第２００２／００１０７９０（ＵＳ，Ａ１）
特開２００１－２６５６５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
G06F 3/06
G06F 12/00