



基礎から学ぶ

ストレージ・ネットワークング

BROCADE

※本記事はブロードコムコミュニケーションズシステムズ株式会社が執筆し、@IT情報マネジメント(<http://www.atmarkit.co.jp/im/>)に掲載された記事を加筆・修正(図版は転載)したものです。

目次

1.	なぜストレージをネットワーク化するのか -----	1
2.	ストレージ・ネットワークの技術 -----	5
3.	ストレージ・ネットワークの導入 -----	12
4.	ストレージ・ネットワークの管理 -----	17
5.	ストレージ・ネットワークの拡張 -----	23
6.	ストレージ・ネットワークはどこへ向かうのか -----	29

1. なぜストレージをネットワーク化するのか

本連載の目的

私たちの今日の生活が IT によって支えられているということは、もはや説明するまでもない事実だ。この IT をインフラとして支えているのが「ネットワーク」と「ストレージ」である。

PC やサーバだけではなく、携帯電話、PDA、そしてストレージ装置に至るまで、あらゆるコンピュータが「ネットワーク」で接続され、互いにやりとり(すなわち「通信」)を行い、そしてテキスト、画像、音楽、映像などあらゆる種類のデータがこのネットワークを通じて「ストレージ」(記憶装置)の中に格納されている(図 1)。

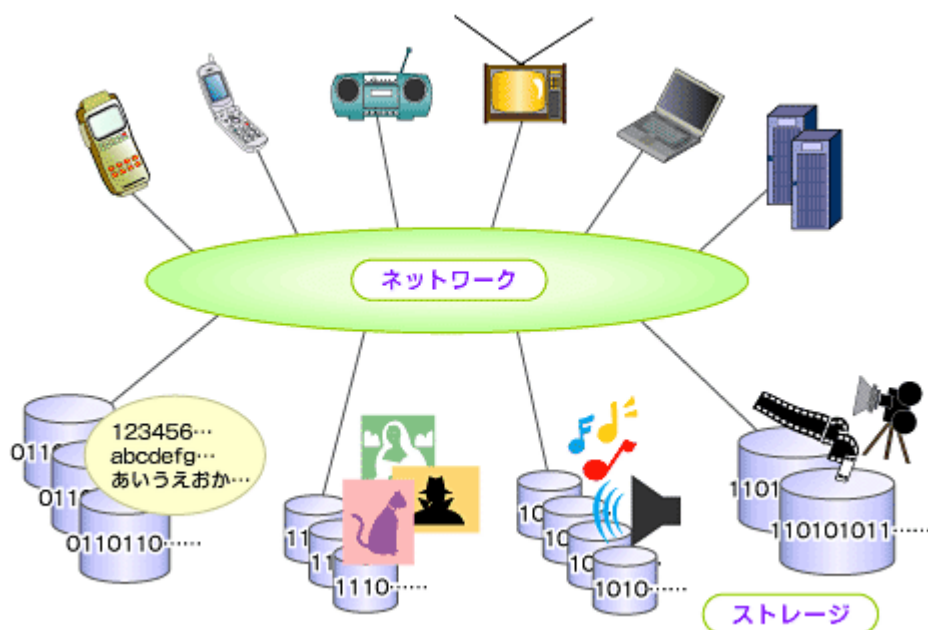


図 1 あらゆるコンピュータはネットワーク経由でストレージを活用している

本連載では、このようにストレージが接続されるネットワークを「ストレージ・ネットワーク」と呼び、その用途や技術、導入・運用に至るノウハウやその価値などを解説していく。ストレージ・ネットワークとは、その名の通り、ネットワークとストレージを結び付けるものであるから、やはり IT インフラにとって重要な概念であるといっていだろう。

本連載では、ストレージ・ネットワーク導入における準備から設計、設置および設定、運用管理、さらに拡張フェーズに至るそれぞれの段階で、「何が大切なのか」「どのようなことを考慮すればいいのか」を解説する(表 1)。

回数/タイトル	内容
第 1 回 「なぜストレージをネットワーク化するのか」	・本連載の目的 ・ストレージネットワーク導入の目的(バックアップ、ディザスタリカバリなど) ・導入におけるメリットとデメリット
第 2 回 「ストレージ・ネットワークの技術」	・DAS、NAS、SAN ・プロトコル:FC-SANとIP-SAN
第 3 回 「ストレージ・ネットワークの導入」	・ネットワークストレージ導入の前提 ・ストレージ・ネットワークと「上手に」つきあうために
第 4 回 「ストレージ・ネットワークの管理」	・ストレージ・ネットワーク管理手法の紹介
第 5 回 「ストレージ・ネットワークの拡張」	・ストレージ・ネットワークが拡張する背景 ・拡張における手法とメリット・デメリット
第 6 回 「ストレージ・ネットワークはどこへ向かうのか」	ストレージネットワークに関する最新技術の可能性と注意点(WAN 高速化装置、仮想化、ILM、ユーティリティコンピューティングなど)

表 1 本連載の構成

また、現在この分野で話題になっている技術にも焦点を当て、単なる紹介ではなく、もっと本質的に読者の方々が理解できるように説明を加える。技術的な内容もさることながら、運用担当者やマネージャ層の視点で、ストレージ・ネットワークの導入、運用の意義について言及したいと考えている。

「ストレージ・ネットワーク」という言葉は、一般的には「SAN(ストレージ・エリア・ネットワーク)」と呼ばれているものに近い。しかし本連載ではあえて「SAN」という技術用語ではなく「ストレージ・ネットワーク」という、より抽象的な表現を用いたい。というのも「SAN」と表現してしまうと「ファイバチャネル」「IP-SAN」「バックアップ」など、巷(ちまた)で広くいわれているキーワードが読者の頭の中に思い描かれてしまうと考えるからである。筆者としては、そのような予備知識をあえて排除し、あらためてストレージ・ネットワークというものを、読者に客観的に見直してもらいたいと考えている。

本連載では原点に戻って「ストレージ・ネットワーク」を解説するつもりであり、技術的なあるいはノウハウとしてのバックグラウンドをお持ちの読者の方々にとっては記述が冗長的に思われる部分もあるかもしれない。この点はあらかじめご了承ください。幸いである。

連載第 1 回となる今回は、いまさらと思われるかもしれないが「そもそもなぜストレージ・ネットワークが必要なのか」ということをあらためて考えてみたい。なぜストレージを「ネットワーク化」することが求められるのだろうか。そこには当然、何らかの理由がある。そこで、まずは「ストレージをネットワークで接続する」ということの本質的な意味を考えてみたい。

ストレージのネットワーク化はなぜ必要？

そもそも「ネットワーク」は、前述のとおり、接続されたモノ同士が何らかの「やりとり」つまり「通信」を行うニーズがあるからこそ、構成されるものだ。現在インターネットに接続されていない IT 機器(サーバやクライアント)はほとんどないといっているが、それはネットワークに参加することで、ほかの機器から情報(データ)を入手したり、逆に提供したりすることができるという、非常に大きなメリットを享受できるからである。

ストレージ・ネットワークに関しても同様に考えることができる。ストレージ・ネットワークではストレージが、ホストとともにネットワークにより接続される。これによってもたらされるメリットとは、例えば 1 台のホストが複数のストレージにアクセスできるようになり、また複数のホストで 1 台のストレージを共有することである。さらにストレージ間で自由にデータを移動してストレージ変更をもっと簡単に行い、OS やアプリケーションをホストから切り離して外部ストレージに格納することで、ホストも自由にスケールアップすることが可能になる。つまり、ストレージをネットワーク化することで、ホストとストレージの関係は「1:1」あるいは「1:n(もしくは n:1)」から「m:n」に変わる(図 2)。

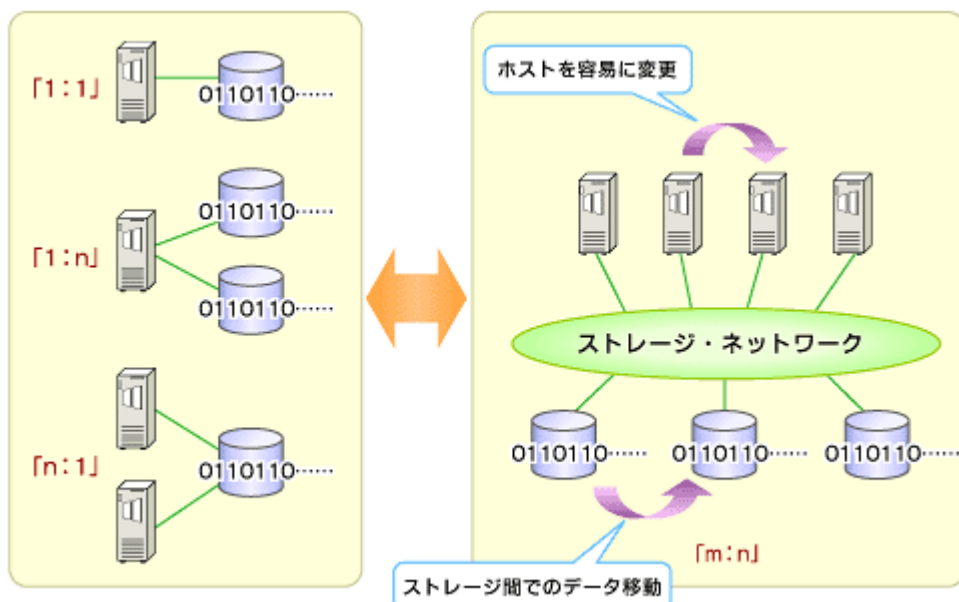


図 2 ネットワーク化でホストとストレージの関係は「m:n」に変わる

ネットワーク化することの本質は、この「関係性」の変化であるといっている。ホストは自由にストレージを選択し、ストレージも自由にホストに割り当てることができるようになる。「m:n」へ関係が変化することで、インフラに柔軟性をもたらすことができるのである。

「m:n」の関係性を構築したいのならば、ストレージはネットワーク化すべきだ。例えばテープ装置は常時稼働しているわけではないから、ホスト1台ずつに対して台数分個別に接続するよりも複数のホストで共有する形態の方が、トータルでのコストが抑えられ、テープ装置をより有効に活用できるといえるだろう。

ストレージ・ネットワークでは、ホストとストレージがその構成要素となる。従って、ストレージに求められる役割やストレージの重要度が高くなればなるほど、より高い柔軟性が求められる。前述のとおり、今日あらゆるデータがストレージに格納されているという現実をかんがみると、ストレージをネットワーク化するのは必然とさえいえる。

ストレージ・ネットワークも「ネットワーク」であるから、その上で通信するモノ同士の間では何らかの「プロトコル」(通信手順)に従って通信を行う必要がある。ファイバチャネルや iSCSI などがそれに該当するわけだが、プロトコルに関する詳細は次回解説する予定である。

ストレージのネットワーク化で得るもの、失うもの

ストレージ・ネットワークを導入するメリットは、前述した導入の目的を振り返ってみれば、おのずと明らかになる。前述のようにホストおよびストレージに「柔軟性」をもたらすことが、ストレージ・ネットワークの本質であり、特徴である。逆説的にいえば、「柔軟性」を必要としないのならば、ストレージ・ネットワークを構成する必要もない。「バックアップ統合」「ディザスタ・リカバリ」などよくいわれる「SAN ソリューション」は結局、この柔軟性から派生するものである。大切なのはソリューションを知っていることよりも、ソリューションを可能とする本質を理解することだと筆者は考える。

ストレージ・ネットワークの導入にも、やはりコストが発生する。それはホストアダプタ(コンピュータを SAN に接続するためのアダプタ)や SAN スイッチ、ソフトウェアを購入するのに必要なコストである。前述の SAN 導入におけるメリットを、費やしたコスト以上に感じるができなければ、結局はそのコストが「デメリット」と認識されてしまう。

「SAN(ストレージ・ネットワーク)はコストが高い」といわれるが、本当にそうなのだろうか。ここで言及している「コスト」について考える際には、「初期コスト」と「ランニングコスト」を厳密に区別する必要がある。

ストレージ・ネットワーク導入においては導入コスト、つまり初期コストがプラスアルファとして掛かるかもしれないが、ランニングコストは導入しない場合に比べて、大幅に低下するかもしれない。「TCO」(Total Cost of Ownership)や「ROI」(Return On Investment)は使い古された言葉ではあるが、投資を行ううえではあらためて考慮する必要がある。もしかするとランニングコストは初期コストなどとは比較にならないくらい大きいものかもしれない(図3)。

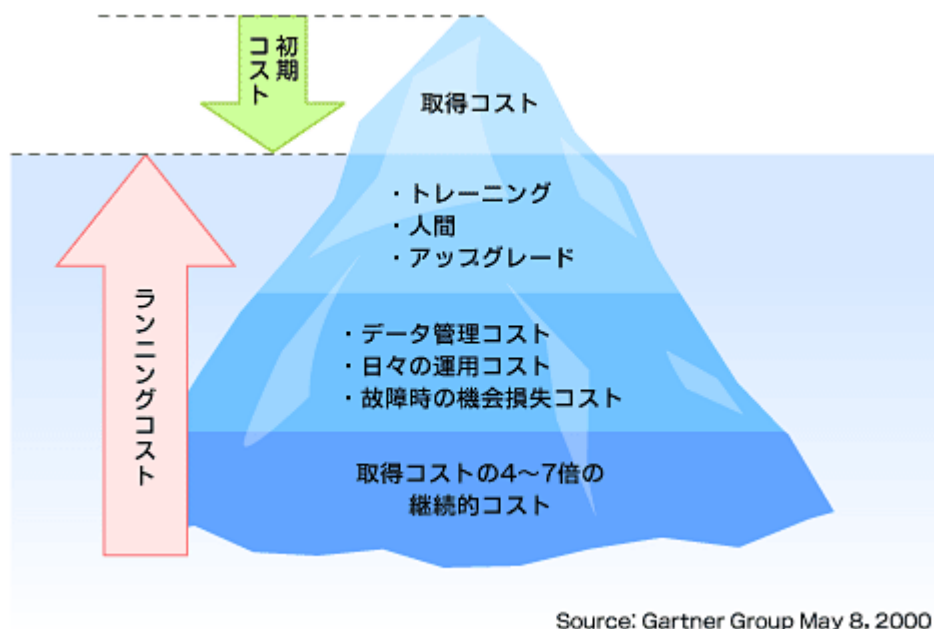


図3 ランニングコストは初期コストより大幅に高くなり得る

もちろん、これは使用形態や運用形態等によって変わってくるため一概にはいえないが、大切なのはコストをより広くとらえ、自分たちのシステムの「本当の」コストを知ることだ。そうでないと「ストレージは高い」「SAN(ストレージ・ネットワーク)は高い」といった、漠然とした議論に終始

するだけでせっかくのメリットを見逃してしまう。ランニングコストは「計算できない」ともいわれるが、多くの場合「計算していない」だけなのではないだろうか。

IT 投資において「サーバ台数はどのくらいになるのか」「ストレージ容量はどのくらい必要か」「新しい技術が出てくるのではないか」など、多くの不確定要素が存在する。ストレージ・ネットワークによって IT インフラに柔軟性を持たせておくことで、このような不確定要素にも柔軟な対応が可能となる。

今回は「ストレージ・ネットワークの技術」として、DAS(Direct Attached Storage)、NAS(Network Attached Storage)および SAN の技術的な特徴と、ストレージ・ネットワークで使用されるプロトコルに関して紹介していく。

2. ストレージ・ネットワークの技術

DAS、SAN、NAS の違い

DAS、SAN、NAS の関係を示すと図 1 のようになる。DAS はストレージをネットワーク化せずに、サーバとストレージを直結する形態、または直接接続されたストレージ装置を指す。主に後述する SAN と対比する用語として用いられており、SAN が登場する以前は基本的にすべてこの形態であった。

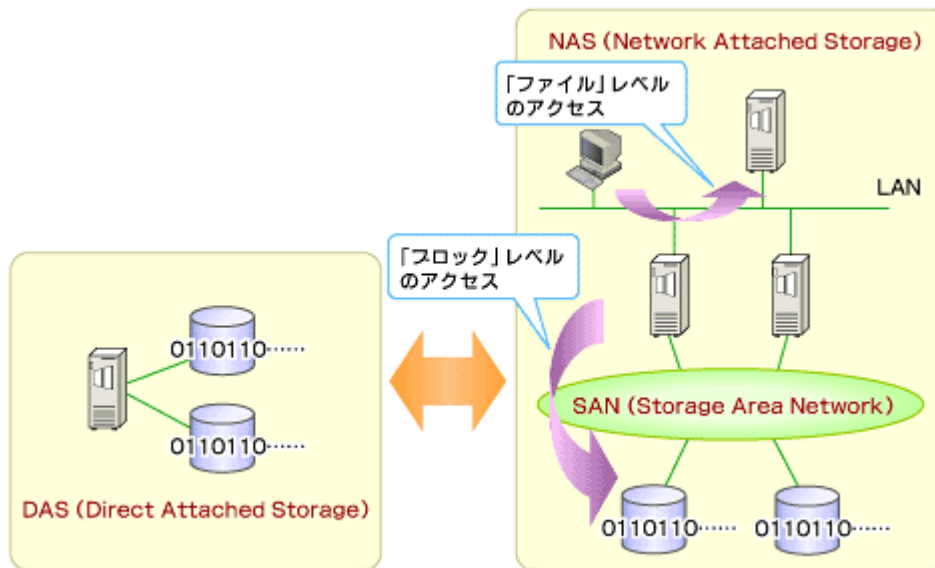


図 1 DAS、SAN、NAS の関係

DAS におけるサーバとストレージの関係性は、前回紹介したように「1:1」または「1:n」となる。単一のサーバが単一もしくは複数のストレージを占有しており、複数サーバでストレージを共有することはできない。従ってサーバ台数の増加やサーバでのストレージ容量の不足に応じて、ほかのストレージの空き容量に関係なくストレージ投資が発生する。ストレージ装置間で利用率が平準化されず、結果として「無駄」が大きいといえる形態だ(図 2)。

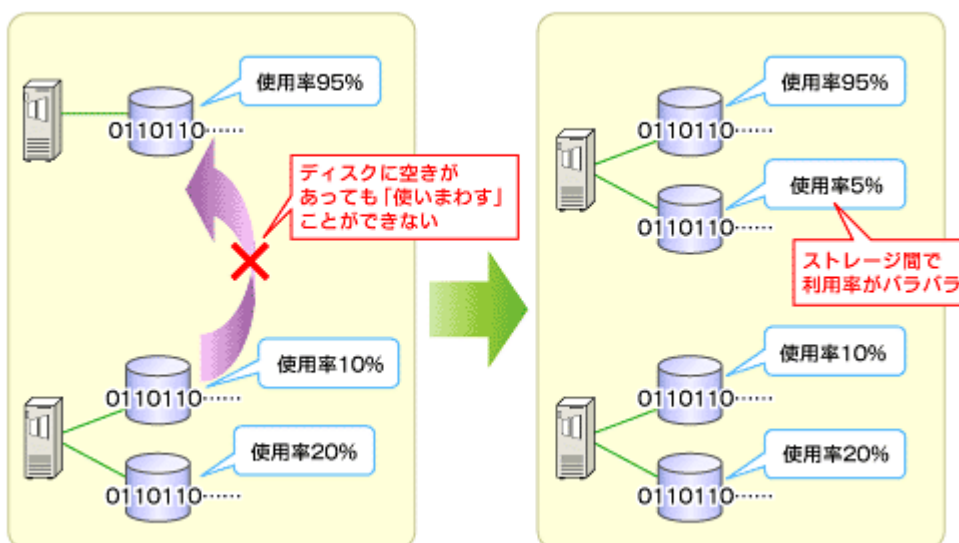


図 2 DAS ではディスクスペース利用が非効率になりやすい

サーバ台数やストレージ容量の増加見込みが限定的、もしくは将来の追加投資がないと導入当初に確定できるようなケースでは、初期コストが低い DAS を選択するメリットはある。とはいえ企業経営と IT がますます密接化し、IT インフラに求められる役割が今後さらに大きくなっていくことが予想される中で、サーバやストレージの将来投資を限定するのは賢明とはいえない。

また日常の運用・監視という観点からすると、DAS ではサーバとストレージ間の通信で「何が起きているのか」をネットワークレベルで把握することができない。一方、SAN の場合はサーバとストレージの間に位置するスイッチから、パフォーマンスやエラーなどに関する情報を取得することができる。SAN を監視のための「窓」として使用するわけだ(図 3)。

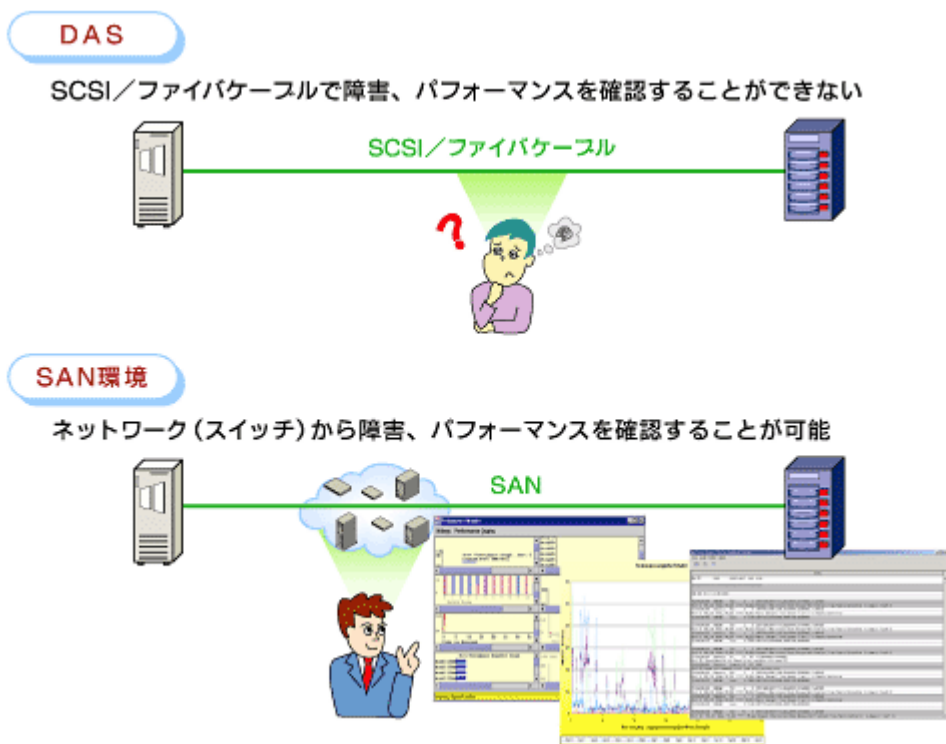
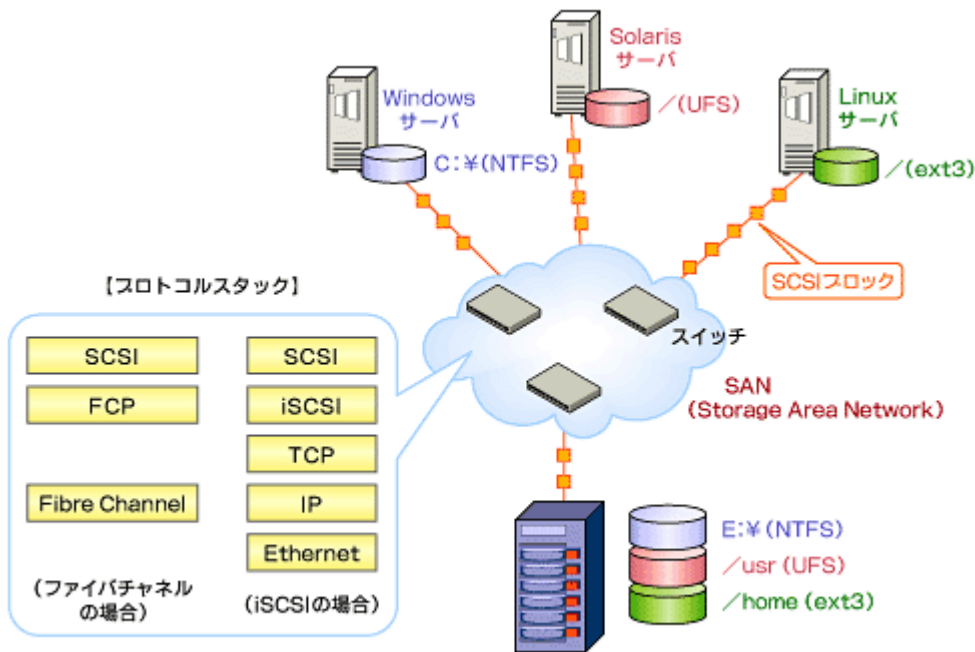


図 3 パフォーマンスやエラーの監視における DAS と SAN の違い

SAN は、スイッチなどを使用してサーバとストレージを結び付ける「ネットワーク」を指す用語である。繰り返すが、「ネットワーク」であるということに注意されたい。SAN 自体はその上に位置するプロトコルやファイルシステムを意識しない。オープンシステムでは、SCSI プロトコルを用い、データを「ブロック」という単位でストレージに対して読み書きするのが一般的だが、SAN ではファイバチャネル(Fibre Channel: FC)や IP プロトコルを SCSI プロトコルと対応づけることで、SAN 内でデータの読み書きを実現することができる。

従って、SAN は「ブロックレベルの通信を仲介するネットワーク」と表現できる。上記のとおり SAN はファイルシステムに対して透過的で、サーバは自身が認識できるファイルシステム(Windows であれば NTFS、Solaris であれば UFS など)でストレージ内のボリュームをフォーマットし、SAN の先に存在する外部ストレージに内蔵ディスクと同じようにアクセスできる(図 4)。



FCP (Fibre Channel Protocol):ファイバチャネルとSCSIを対応させるプロトコル

図 4 SAN では SCSI のデータブロックをネットワーク経由で送ることができる

ただ、NTFS や UFS といったファイルシステムはサーバごとに存在し、単一ボリュームを複数サーバから同時にアクセスできるように構成できない。これを可能にするために、複数サーバでボリュームを共有する SAN 対応のファイルシステムなどが提供されている。この場合は、サーバ間のアクセスを管理するサーバなどが別途必要となる。

NAS はその名のとおり、「ネットワークに接続された」ストレージ装置だ。ここでいう「ネットワーク」とは「IP および Ethernet」であり、SAN とは違って「ファイル」単位でのアクセスが基本になる。つまり、クライアントは IP ネットワークを経由して NAS に存在するファイルにアクセスする(図 5)。

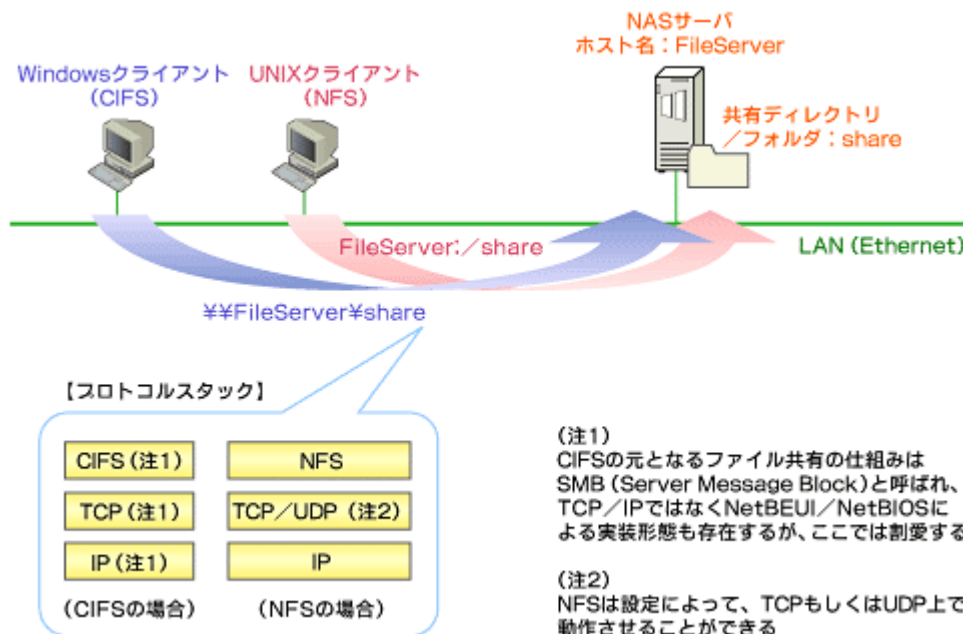


図 5 NAS はネットワーク経由でファイル単位のアクセスを実現する

ファイル共有システム(プロトコル)として代表的なのは、Windows 環境で使用される CIFS(Common Internet File System)と、主に UNIX および Linux で使用される NFS(Network File System)である。これらは IP ネットワーク上で動作するクライアント・サーバ型のプロトコルで、サーバ(つまり NAS)側で排他制御などのファイル管理を行っている。従って NAS の場合、SAN 環境にはないファイル単位での排他制御や同時アクセスが可能である。ただしファイルをアクセス単位とする NAS においては OS のファイルシステム処理が加わるため、パフォーマンスという観点で比較すると、ブロックアクセスを前提とする SAN に比べるとオーバーヘッドが大きい。

「SANとNASはどちらが優れているのか」と両者を比較しているケースがしばしば見受けられるが、これは「ネットワーク(SAN)」と「ストレージ(NAS)」という全く異なった技術を比較していることであり、本質的には意味のない議論だ。また NAS は、クライアント側へ提供するインターフェイスは CIFS もしくは NFS というファイルレベルのアクセスだが、NAS 自体のストレージへのアクセス(こちらはもちろんブロックレベルのアクセスとなる)の手段として SAN を用いることができる(図 6)。この場合、NAS サーバ筐体内のストレージ容量に限定されることなく、ストレージを効率的に拡張していくことが可能になる。このように SAN と NAS は対立するものではなく、補完し合う技術と考えるべきだろう。

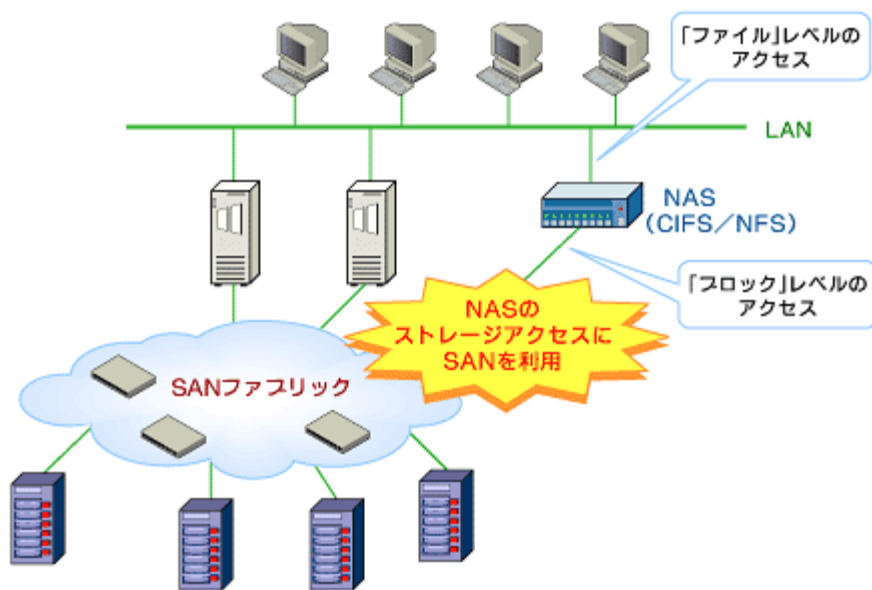


図 6 SAN と NAS は単純に比較できない技術

ファイバチャネル SAN の進化

SAN で使用されるプロトコルで、現在主流となっているのが「ファイバチャネル」である。ファイバチャネルは ANSI(米国規格協会: American National Standard Institute)の T11 委員会で、1988 年に規格化が開始された。当初からギガビット/秒クラスのデータ通信を想定しており、高速かつ信頼性の高いデータ伝送に適した設計になっている。ファイバチャネルプロトコルは FC-0 から FC-4 までの 5 階層から構成されているが(表 1)、これらはすべてハードウェアによって処理され、サーバ CPU への負荷は低い。

FC レイヤ	役割	対応する技術要素(主なもの)
FC-4	上位プロトコルとのマッピング	FCP(Fibre Channel Protocol) FC-ATM FICON(FIbre CONnection)
FC-3	共通サービス	
FC-2	フロー制御	フレーム/シーケンス/エクスチェンジ CoS(Class of Service)
FC-1	符号化・復号化	8B/10B 64B/66B
FC-0	物理的なインターフェイス	1/2/4/8Gbps FC 10Gbps FC SC, LC, DB9

表 1 ファイバチャネルのプロトコル階層

ファイバチャネルのインターフェイス速度は、1Gbps、2Gbps を経て、現在は 4Gbps が主流であり、HBA (Host Bus Adapter: コンピュータに装着するファイバチャネル通信のためのインターフェイス) やファイバチャネル・スイッチ、ストレージ装置のインターフェイスが続々と 4Gbps に対応している。さらに 2007 年から 2008 年にかけて 8Gbps に対応した製品も出始めており、今後数年のうちに 8Gbps ファイバチャネルが普及することが予想される。

ファイバチャネルには 10Gbps のインターフェイス規格も存在する。ただ 1/2/4/8Gbps と 10Gbps のファイバチャネル規格の間には下位層のレベルで互換性がなく、両者の間では物理的なポートを共有することができない。このためコスト面で不利となる 10Gbps ファイバチャネルは現在、一部の FC スイッチでスイッチ間の接続に使用される程度で、広くは普及していない。

ファイバチャネルでは「フレーム」という単位でデータを伝送する。またファイバチャネルは FC-4 層でさまざまな上位プロトコルとの対応付け (マッピング) を可能としており、SCSI-3 を FC にマッピングする FCP (Fibre Channel Protocol) や IP を FC 上で通信する IPFC (IP over Fibre Channel)、メインフレーム通信用の FICON (Fibre CONnection) などが規定されている。

ファイバチャネルでは 24 ビットのアドレス体系が採用され (ファブリックポロジーの場合)、接続するデバイスへ自動的にアドレスが付与される。ファブリックポロジーではネームサービス等の各種機能も自動化され、システム管理者がそれらを意識する必要はない。

IP で SAN を実現する FCIP と iSCSI

IP-SAN に関連する技術として、ここでは「FCIP」(Fibre Channel over IP) と「iSCSI」(Internet SCSI) を紹介する。

FCIP は RFC 3281 で規定され、ファイバチャネルフレームを IP パケットでカプセル化する技術である。FC-SAN 同士を IP ベースの WAN 回線で結び、ディザスタリーカバリ (災害復旧) サイトを構築する際に利用される (図 7)。ここで IP は「トンネル」としての役割のみを果たしており、IP ネットワーク越しにファイバチャネルをそのまま利用することができる。FCIP はファイバチャネルを IP で補完する技術という位置付けである。

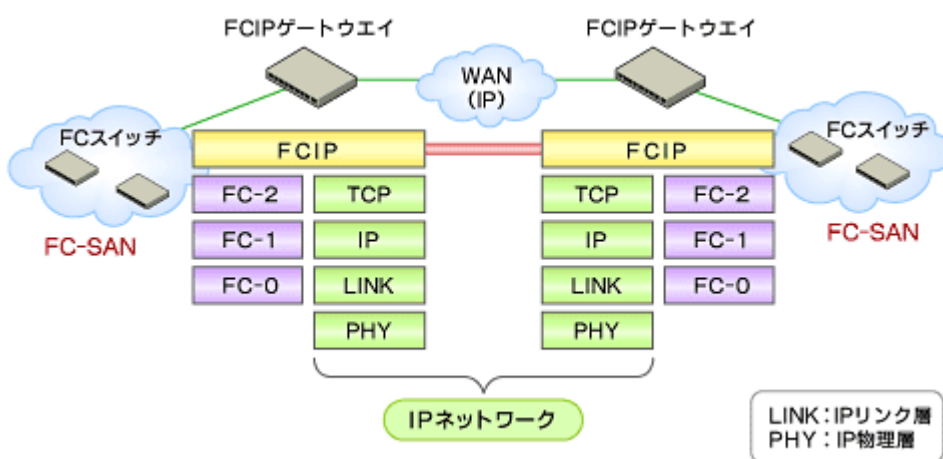


図 7 FCIP ではファイバチャネルフレームを IP にカプセル化する

一方、iSCSI は RFC 3385 などで規定され、TCP/IP プロトコル上で直接 SCSI ブロックを伝送する技術である。TCP/IP をベースにしているためにファイバチャネル対応の HBA やスイッチが不要で、FC-SAN を補完する技術といえる (図 8)。iSCSI では OS ベンダなどが提供するイニシエータにより、ソフトウェアでプロトコル処理を行うことが可能だ。しかし、データ I/O 処理をソフトウェアで行うとサーバ CPU の負荷が大きくなるので、これをハードウェア処理で回避する TOE (TCP/IP Offload Engine) が提供されている。

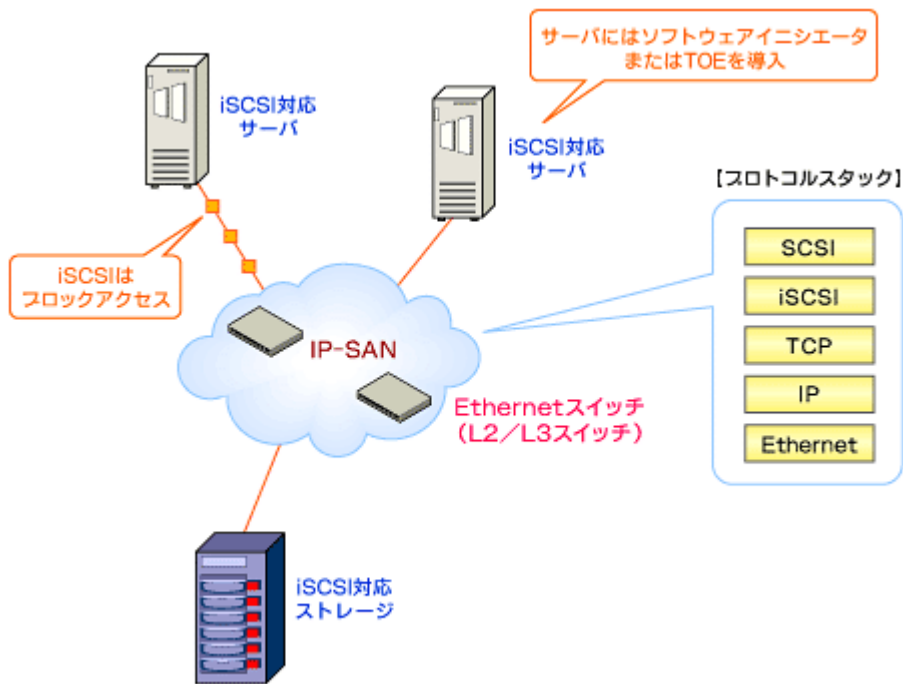


図 8 iSCSI は TCP/IP 上で SCSI ブロックを直接伝送する

iSCSI による IP-SAN は、FC-SAN に比べてコストが安いといわれている。確かに FC-SAN に比べると HBA や FC スイッチなどのハードウェア投資が抑えられるためコストは安くなるが、近年は FC 製品の価格下落も激しく、両者のコスト差は小さくなってきている。また iSCSI には TCP/IP を使用することによるオーバーヘッドも存在するため、パフォーマンスとコストを総合的に判断したうえで、用途に応じてファイバチャネルと iSCSI を使い分けるというのが賢明な判断だろう。また、iSCSI とファイバチャネルデバイス間の通信を可能にする「ゲートウェイ」製品を提供しているベンダもあるので、参考にしていきたい。

今回は「ストレージ・ネットワークの導入」と題して、ストレージ・ネットワーク導入に際して前提となる事柄や、ストレージ・ネットワークをより上手に活用するために導入前に検討しておくべき事項などを紹介する。

3. ストレージ・ネットワークの導入

ネットワークストレージ導入の前提

「ネットワークストレージを導入する」とはどういうことなのだろうか。この問いに答えるため、ネットワークストレージの導入における筆者の考えるフローを図1のようにまとめてみた。ここではこの図に従って説明していきたい。

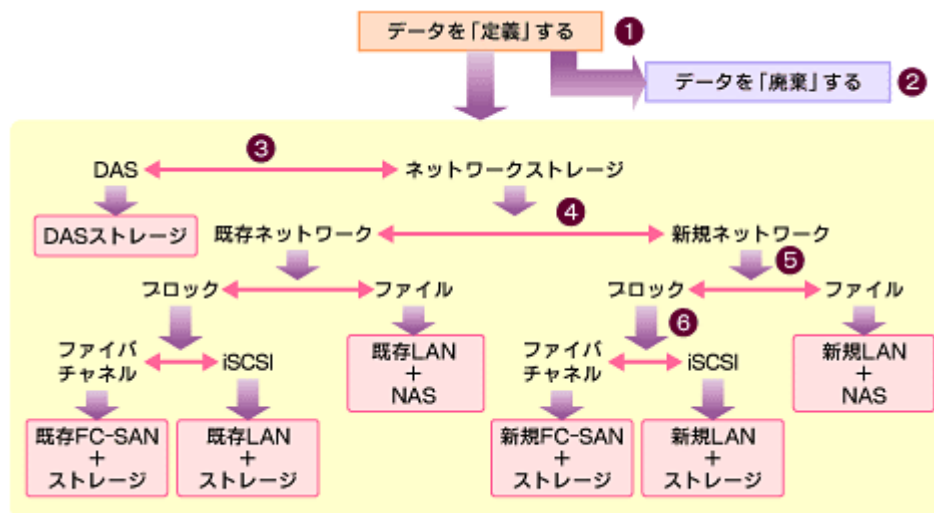


図1 ネットワークストレージ導入のフロー

ストレージの導入において何にも増して大切なことは、そこに格納されるデータを定義することである(図1の1)。ストレージは器であり、ストレージ・ネットワークはそこへ至るための通路に過ぎない。「誰が」「いつ」「何のために」「どのように」使用するデータなのかを確認し、そのデータが持つ価値を再認識することが、ネットワークストレージ導入の出発点となる。

自分たちが格納しようとしているデータについて知ることができれば、そこへ至る経路(ネットワーク)と器(ストレージ)は自ずと選定できる。データ定義はそのデータが持つ価値を理解していなければ行えないため、そのデータを使用しているユーザーでなければ実施できない、業務に直結した作業である。以下ではこのデータ定義について、より詳しく触れていこう。

データを定義する際には、サービスレベルとパフォーマンスという2つの指標で考えるとよい。

サービスレベル指標とは、そのデータに関わる業務の耐障害性に関する指標で、「RTO」(Recovery Time Objective: 目標回復時間)と「RPO」(Recovery Point Objective: 目標回復ポイント)に代表される。RTOとRPOは短ければ短いほど望ましいが、その分コストがかかる。したがって両者のバランスを考える必要がある(図2)。またRTOとRPOを規定しておけば、「DR」(Disaster Recovery: 障害復旧)システムを導入する際の要件定義にも直結する。

- RTO (Repair Time Objective : 目標回復時間)
 - ・システム復旧までにかかる時間を規定
 - ・RTOはシステムの機会損失の大きさにより変化
 - ・短ければ短いほどよい
- RPO (Repair Point Objective : 目標回復ポイント)
 - ・業務を再開するためにどの時点からのデータをリカバリする必要があるかを規定
 - ・RPOはデータに求められるリアルタイム性により変化
 - ・短ければ短いほどよい

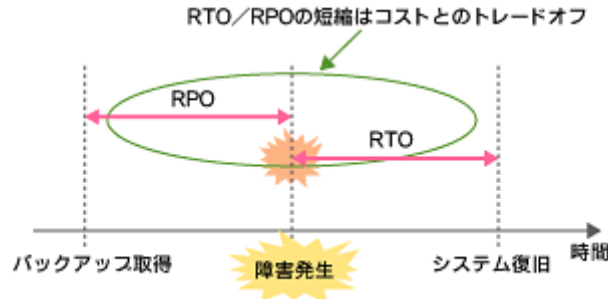


図 2 RTO と RPO

一方、パフォーマンス指標とはストレージ・ネットワークも含めた業務システム全体のパフォーマンスに関する指標で、システムのレスポンスタイムやストレージの IOPS (単位時間当たり入出力: Input/Output per second) に代表される。ここでは通常時だけでなく、縮退時のパフォーマンスも検討しておくとい。縮退時には通常時より低いパフォーマンスでも許容されることが多く、通常時と縮退時でインフラのレベルを変えることができるからである。

データ定義においては、そのデータが持つ「価値」だけではなく「リスク」に関する検討も必要だ。「データを持つ」ということは企業の競争力を高める上で必須の要件であるが、一方で価値があるが故にそのデータを奪われるリスクも存在する。データを持つことのメリットと、データを持つが故に引き受けなければならないリスクを比較したうえで、リスクの方が大きいという結論に至れば、そのデータは廃棄すべきということになる(図 1 の 2)。このようにデータを中心に考えることで、不必要なインフラ投資を抑えることも可能である。

また、データ定義に際してはデータの瞬間的な価値だけでなく、時間経過に伴う価値の「変化」も併せて検討することが望ましい。データには新鮮さが求められることが多く、データの価値は時間の経過と反比例の関係にあるのが一般的だ。従って、時間経過によるデータ価値の変化に応じて、適切なストレージに格納するとよい。

データ定義の結果、データを保持しておくべきという結論が得られれば、それを格納するストレージとそこへ至るネットワークの選定作業に入る。既存ストレージが存在し、データ定義の結果そこへ格納すればよいというケースもあるが、今回この部分は省略する。まず検討すべきは、「DASにするか、それともネットワークストレージにするか」という点だ(図 1 の 3)。DAS のメリットとデメリットは前回紹介したのでここでは省略するが、データ定義の結果、データ格納先として DAS が望ましいのであれば、それも 1 つの解である。

DAS が選択されない場合にはネットワークストレージが選ばれるわけだが、ストレージおよびネットワークは必ずしも新規に必要となるわけではない(図 1 の 4)。既存でネットワークインフラが存在するならば、できる限りそれを使うべきだろう。既存ネットワークでも新規ネットワークでもその後の手順に違いはないため、新規ネットワークを導入する前提で話を先に進める。

前回紹介したように、ストレージ・ネットワークは大きく「ブロック」アクセスと「ファイル」アクセスに分けられる(図 1 の 5)。ファイルアクセスのストレージ・ネットワークを選んだ場合、「(新規) LAN+NAS」という結論に至る。例えば、格納するデータがオフィス文書系のドキュメント中心で、それらをファイルレベルで共有したいという場合は、LAN と WAN を使用してデータを NAS に格納するという選択が有効だ。

ブロックアクセスが求められる場合は SAN 導入を検討することになるが(SAN の定義は前回の説明に従う)、ここでは「ファイバチャネル(FC-SAN)か iSCSI(IP-SAN、実際には LAN)か」という選択になる(図 1 の 6)。ここでも既述のデータ定義の結果に従い、格納するデータに求められる信頼性、アクセス速度や頻度、コストなどの兼ね合いで決定する。

再度確認しておくが、ここでいう「コスト」とは初期コストだけではなく、ランニングコストも含めたトータルコストのことだ。初期コストはいうまでもないが、ランニングコストの一例を挙げると図3のようになる。トータルコストとはあくまでも「イニシャルコスト+ランニングコスト」であり、第1回で説明したように、ランニングコストの比重が圧倒的に大きいケースがほとんどである。

最終的に導入に至るストレージ・インフラが NAS であろうと FC-SAN であろうと、データを中心に検討を行うことが本質的には重要である。近年よくいわれる「ILM」(Information Lifecycle Management)や既述の DR も、データを定義することから出発するという点では変わらない。「データ」からアプローチすることで、より上手にストレージ・ネットワークと向き合うことができる。

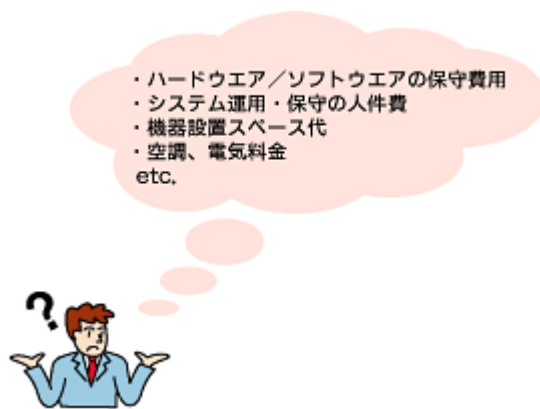


図3 ネットワークストレージのランニングコスト

ストレージ・ネットワークと上手に付き合うために

ストレージ・ネットワークと付き合っていく上で最も大切なことは、データ管理におけるポリシーを確立し、そのインフラとしてストレージ・ネットワークを位置付けることである。ここでもデータを中心としたアプローチを採用し、データの重要度、アクセス頻度といった観点でストレージ・ネットワークを活用する(図4)。

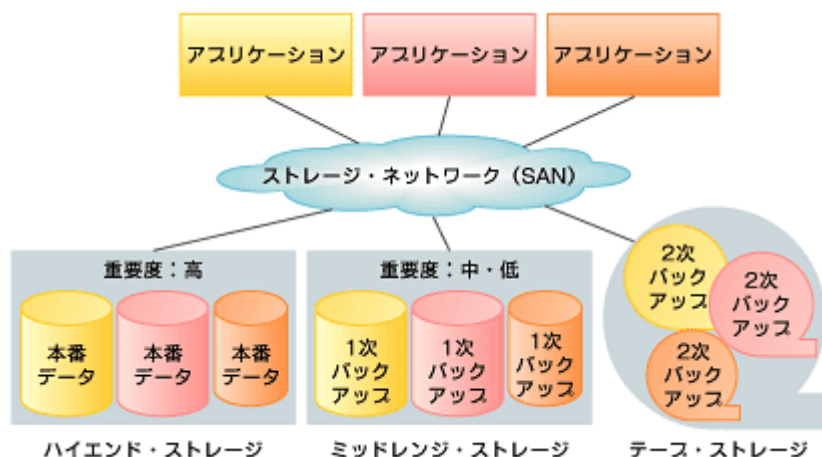


図4 データアクセスポリシーとSANの関係

詳細な説明は省略するが、例えばデータの重要度から上述のサービスレベルポリシーを規定し、そこからストレージに求められる機能要件を導き出すこともできる(図5、表1)。

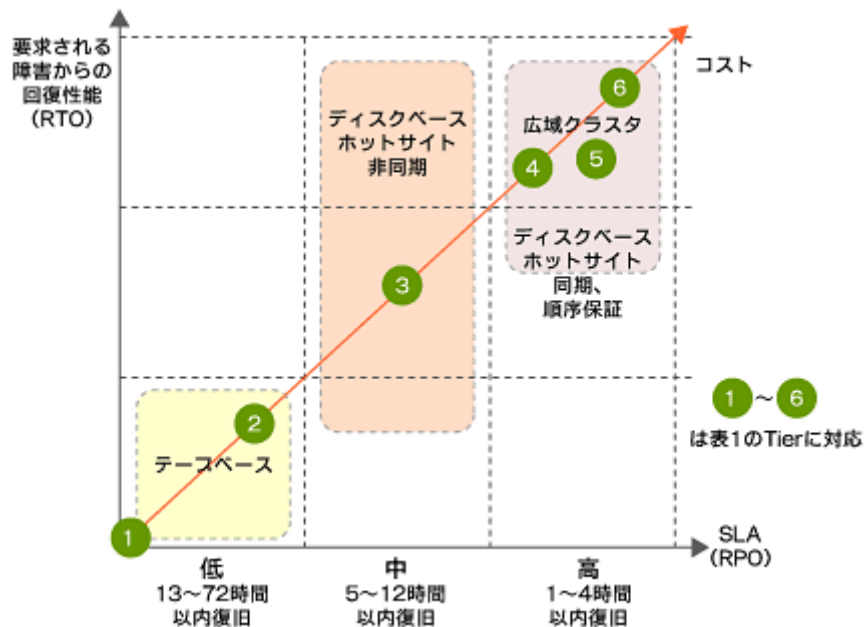


図5 データの重要度に基づくリカバリーポリシー例

	Tier-1	Tier-2	Tier-3	Tier-4	Tier-5	Tier-6
	オフサイト保存	オフサイト保存 / warm サイト	リモートバックアップ / リモートレプリケーション	リモートバックアップ / リモートレプリケーション / warm サイト	2 相コミット	同期 I/O によるゼロデータロスシステム
説明	オフサイトにおけるデータの保存。データの移動は物理的な手段による	オフサイトにデータを保存。保存だけでなく、Warm サイトを構築し、データをインポート	オフサイトにデータを保存。データの移動はネットワークによる	オフサイトにデータを保存。データの移動はネットワークによる。さらに Warm サイトを構築し、データをインポート	オフサイトにデータをミラーリング	完全同期 I/O によるリモートクラスタリング
使用技術 (スナップショットなどを使用する)	通常のバックアップ + 運搬	通常のバックアップ + 運搬 + 手動インポート	SAN/LAN を利用したリモートバックアップ	非同期データレプリケーション	同期式データレプリケーション	リモートクラスタシステム
RTO/RPO	1 週間以内	1 日程度	1 日以内	4 時間以内	1 時間以内	クラスタのフェイルオーバー時間
リカバリーポイント	前回のデータ移動のタイミング	前回のデータインポートのタイミング	前回のバックアップ / レプリケーションのタイミング	前回のデータインポートのタイミング	前回の I/O	前回の I/O
	同期ミラー / スナップショットなし + テープによるバックアップ			同期ミラー / スナップショットあり		

表1 図5の「データの重要度に基づくリカバリーポリシー例」の詳細

ポリシーを定義することは人間の仕事だが、ポリシーを実行するのはストレージ装置やソフトウェアに担当させてよい。格納されてからある一定期間以上経ったデータ、あるいは一定期間以上アクセスされていないデータは自動的にバックアップストレージに移行するといった運用も考えられる。ブロックレベルでもファイルレベルでもこのような処理を自動化するツールが登場してきており、データのライフサイクル管理という観点から検討する余地がある。

ストレージ・ネットワークには柔軟性と拡張性が求められる。ネットワークは幅広く接続できることに存在意義があり、ある日突然サーバやストレージが追加された場合に、ネットワーク側ではそれを許容できなければならない。SAN スイッチをはじめとするネットワーク機器では、ポートキャパシティ管理やネットワーク帯域のパフォーマンス管理が行えるものもある(図 6)。これらを活用することで、システム拡張時や障害時に受動的に対処するのではなく、より能動的にストレージ・ネットワークと付き合い合うことができる。

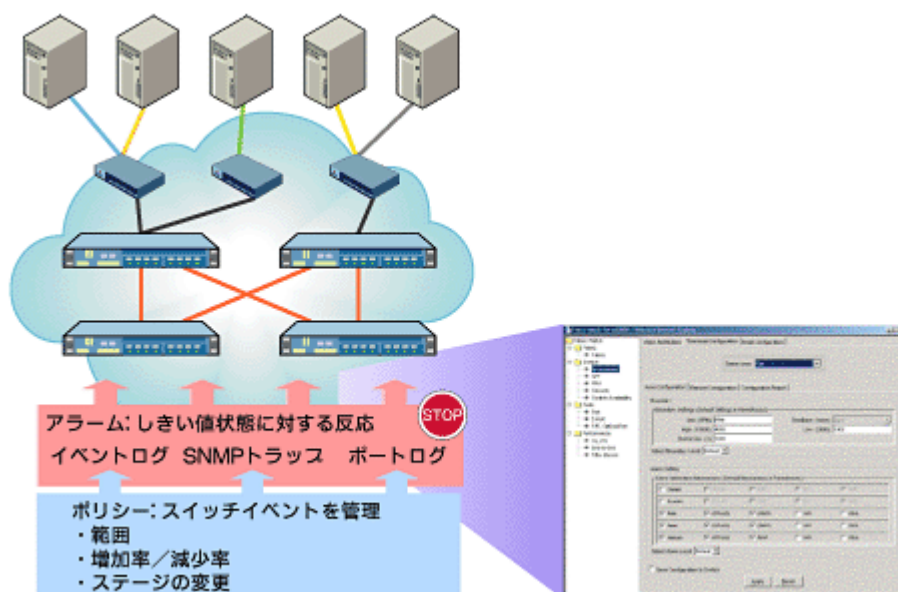


図 6 しきい値ベースのプロアクティブ監視 (Brocade FabricWatch の例)

最後にストレージ・ネットワークを上手に活用するためには、最新の技術動向をチェックすることも忘れてはならない。ストレージの世界でも日進月歩で技術は進化している。ストレージ・インフラは企業活動に影響を受けるので、業務の進捗度合いなどを勘案しつつ、自分たちに関係する技術の動向を見守っていく必要があるだろう。

ストレージは企業活動の根幹を支えているインフラである。データをどのように管理していくかというより大きな視点で、ストレージ・ネットワーク管理というものをとらえていただきたい。

今回はネットワークストレージ導入の本質を解説した。次回は「ストレージ・ネットワークの運用管理」と題して、より具体的なストレージ・ネットワークの管理手法を解説する予定である。

4. ストレージ・ネットワークの管理

ストレージ・ネットワークの管理手法

ストレージ・ネットワークの管理手法にはさまざまなものがあるが、図 1 に示したように SNMP、Syslog、機器の API を使う手法が代表的である。

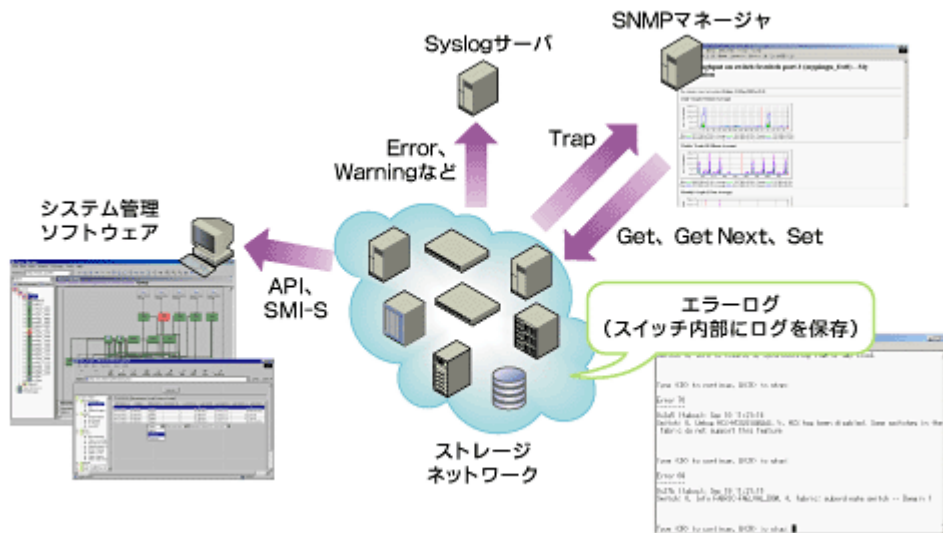


図 1 ストレージ・ネットワークの管理手法

この中で、SNMP (Simple Network Management Protocol) による管理は最もよく使用されているものだ。SNMP は IP ネットワークにおける代表的な管理手法だが、ファイバチャネル(FC)をベースにした SAN 環境でも数多く利用されており、FC スイッチやストレージ装置など SAN ベースの機器のほとんどが対応している(図 2)。

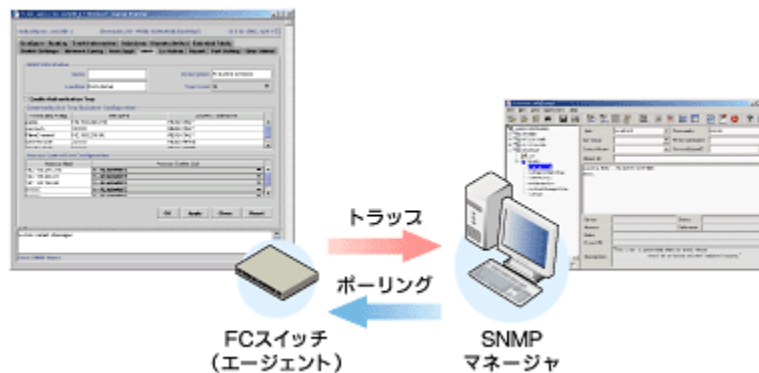


図 2 FC スイッチと SNMP (プロセードのスイッチの場合)

SNMP を用いてストレージ・ネットワークを管理するうえで注意すべきなのが、RFC 1213 で規定され、すべての SNMP 製品が対応する MIB- II (RFC 1213-MIB) は、TCP/IP ネットワークを前提にしており、FC-SAN には対応していないということだ。つまり、MIB- II で IP ネットワークレベルでのトラフィック監視や統計情報の収集などを行うことはできるが、ファイバチャネル・ネットワークのそれらを監視することはできない。そこで、ファイバチャネル製品を取り扱うベンダ各社で構成されている FibreAlliance から FibreAlliance MIB (FC mgmt Integration MIB) が提供されており、これによりファイバチャネル・ネットワークで、各ポートのさまざまな情報を取得することができる。

さらに機器それぞれの独自機能を管理するために、ベンダごとにプライベート MIB も提供されている。ちなみにブロードの場合、Brocade Connect という Web サイトにアクセスして、これらを手入することができる。「SNMP でどの項目を監視するのがいいか」という質問を受けることも多いが、各 FC ポートのスレーブアップ/リンクアップ/ダウンなど、パフォーマンスやエラーに関する項目を監視することを推奨している。これらに関しては、本稿後半でより詳しく解説したい。

UNIX サーバやネットワーク機器の管理手法として一般的な Syslog も、FC-SAN の管理手法としてよく用いられている。SNMP の場合と同様に、FC スイッチなどの機器が「クライアント」となり、Syslog サーバに各種ログを送信する形態である。スイッチのようなネットワーク機器の場合、通常はログが機器内に保存されるため、それぞれのスイッチに個別にログインしなければ、ログを確認することができない。また一定数のログが保存されると、古いものから順に上書きされてしまうこともある。そこで Syslog サーバ (Syslogd) を用意し、そこに各機器からログを送信して一元管理する方法が一般的だ。Syslogd (Syslog デモン) は UNIX 系の OS では標準で提供されており、フリーで利用できる Windows ベースの Syslogd も存在するため(図 3)、比較的容易に利用することができる手法である。

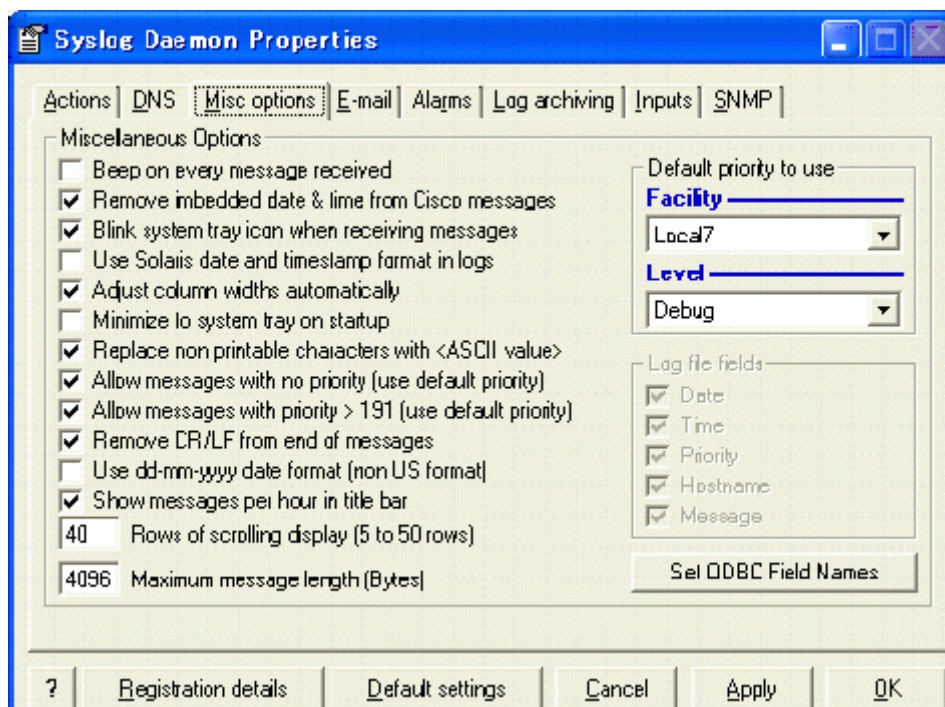


図 3 Windows ベースの Syslogd (Kiwi Syslog Daemon)

アプリケーションソフトウェアからストレージ・ネットワーク全体を管理するために、ストレージやスイッチベンダが提供する API (Application Programming Interface) を用いるのも、これまで一般的に採用されてきた手法である。ただこの場合は、管理アプリケーション(ソフトウェア)側でそれぞれの機器ベンダが提供する API に合わせてソフトウェア開発を行う必要があり、より多くの機器をサポートしようとすればするほど対応する API が増えることになるため、開発効率が悪い。

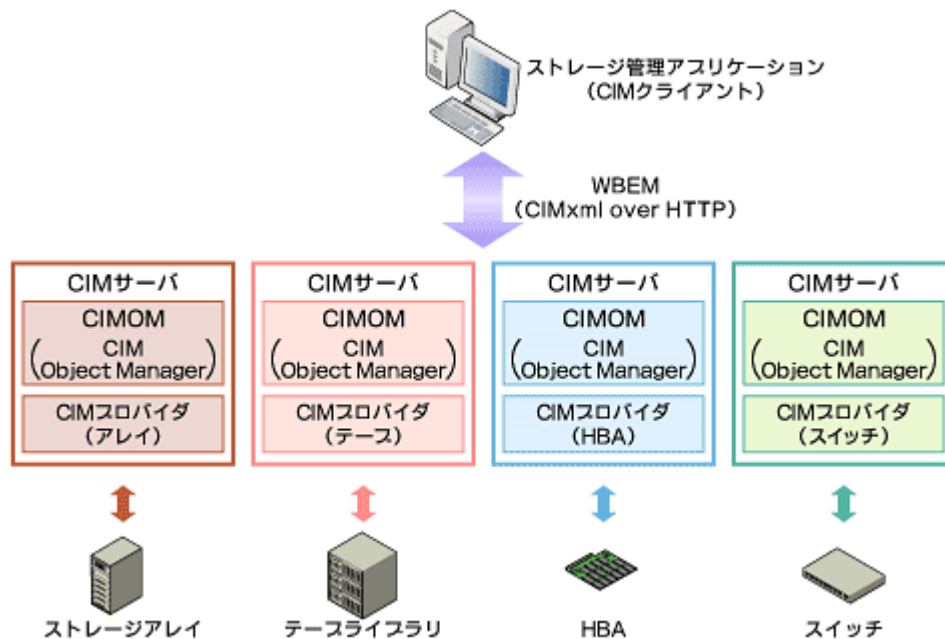


図 4 SMI-S のモデル

このような問題を解決するため、言い換えれば「ストレージ管理の標準として高機能でオープンなインタフェースを提供」するために、ストレージ関連製品の業界団体である SNIA (Storage Network Industry Association) が作成した仕様が、SMI-S (Storage Management Initiative Specification) である。SMI-S は DTMF (Distributed Management Task Force) の CIM (Common Information Model) と WBEM (Web Based Enterprise Management) 規格をベースにしており、ストレージ装置やスイッチなどのデバイスとストレージ管理アプリケーションの間の通信を標準化するものである (図 4)。SMI-S の詳細については、SNIA Japan の Web サイトなどを参考にいただきたい。

ストレージ・ネットワークで何を管理すべきか

ストレージ・ネットワークの管理においてよく聞かれるのが、「一体何を管理すればいいのか」ということだ。一般にシステム運用管理では「構成管理」「変更管理」「性能管理」「問題管理」といった項目が用いられているが、ストレージ・ネットワークの場合でも基本的にこれらに変わりはない。FC-SAN の場合を例に、上記 4 つの管理項目について紹介していこう。

構成管理

ネットワーク機器を構成する物理的および論理的構成を管理することである。当然であるが、常に最新の状態に保つようにしなければならない。物理的なネットワーク構成図や接続構成図などを作成するのはもちろん、各機器の IP アドレスや導入されているライセンス、そのほかにも例えばスイッチであればゾーニング設定、ストレージであれば LUN マスキング設定など、ストレージ・ネットワーク関連の各種設定を把握しておく。いうまでもないことだが、「最新の状態に保つ」ためには次に説明する変更管理を適切に行うことが必須条件である。

変更管理

システムを長期間使用し続けていれば、必然的にさまざまな「変更」が発生する。FC-SAN の場合は特に「ネットワーク」であるため、サーバなどの機器が頻繁に追加されたり、ストレージ装置内部のディスクが追加されたりするようなことも多い。このようにネットワークに何らかの変更が加えられた場合、それらを正確に記述して最新の情報として「構成管理」ができるようにしておかなければならない (図 5)。

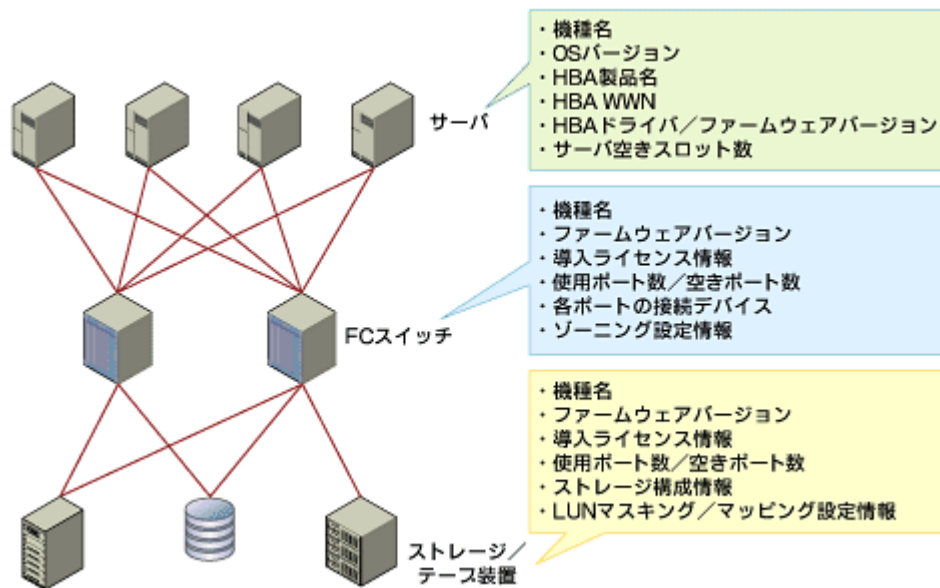


図 5 FC-SAN での構成管理と変更管理の例

性能管理

性能管理としてはパフォーマンス管理が代表的な管理項目だが、これにキャパシティ管理を含める場合もある。FC-SAN においてもパフォーマンス管理は重要な要素である。特定機器からの I/O もしくは特定機器への I/O が集中しているようなケースでは、ネットワークレベルでそれを取り除く必要がある。また、スイッチ同士をカスケードしている構成では、スイッチ間のカスケードリンク (Inter Switch Link:ISL) がボトルネックになる可能性もある。その場合は ISL 本数を増やす、あるいは ISL 間のロードバランスを行えるようにする、といった対策を施すのが有効である (図 6)。

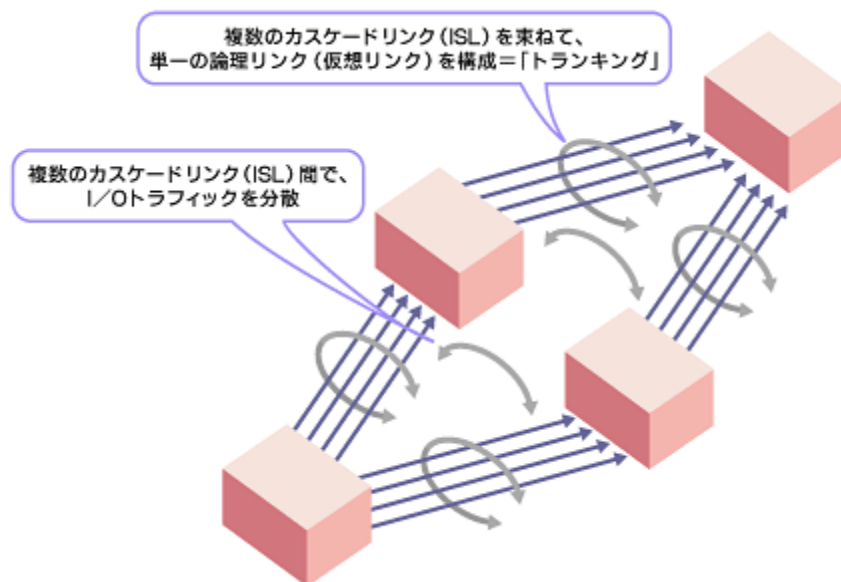


図 6 FC-SAN でのパフォーマンス管理 (プロケードのスイッチの場合)

キャパシティ管理という観点で FC-SAN においてよく問題となるのが、FC ポート管理である。システム拡張に際して SAN にさらにデバイスを接続しようとしても、FC スイッチ側のポート数がすでに足りない、というケースは結構多い。これに対応するためには、空きポートがある一定数を下回った時点でシステム拡張のための施策を取るべきだ。例えば ISL を用いて別のスイッチに接続できるようにする、よりポート数の多いスイッチに買い替える、などである。最近では必要時に追加ライセンスでポートを使用できるスイッチも登場しており、オンデマンドでリソースを追加

することが可能になっている。ストレージ装置では容量管理が代表的なキャパシティ管理の項目だろう。こちらも最近はオンラインでボリューム容量を追加できるものがある。

問題管理

代表的な問題管理の項目は障害管理である。FCスイッチであれば先述したポートのリンクダウンなどの監視に代表されるが、問題を早期に発見できるほど影響は小さくできるため、「予防保守」の観点で管理を行うことが望ましい。例えば FC スイッチでは、電源やファンといった構成要素の状態を把握し、「ファンの回転数が xxxx 回転/分を下回ったら管理者に警告メッセージを出す」などといった運用をしておくことにより、障害の兆候を事前に察知することができる。前回も述べたが、特に障害管理においては、能動的にシステムと付き合うことが望まれる。

問題管理の一環として、昨今注目されているのがセキュリティ管理である。特にストレージ・ネットワークは「データの最終的な格納庫」であるストレージへ至る経路を提供するため、不正アクセスなどへの対策は万全を期す必要がある。ファイバチャネルベースの SAN では TCP/IP ネットワークほど多くの不正アクセス手法は現時点では見つかっていないが、機器の WWN (World Wide Name: ファイバチャネルネットワークにおける機器の識別子) を偽って不正にネットワークに侵入する「WWN スプーフィング」といった手法が広く知られている。従って、アクセス制限を行うゾーニングの技術をより高度化し、あるいはスイッチにおいてデバイス単位で SAN ファブリックへの参加 (ログイン) を制限するといった手法が確立されている (図 7)。

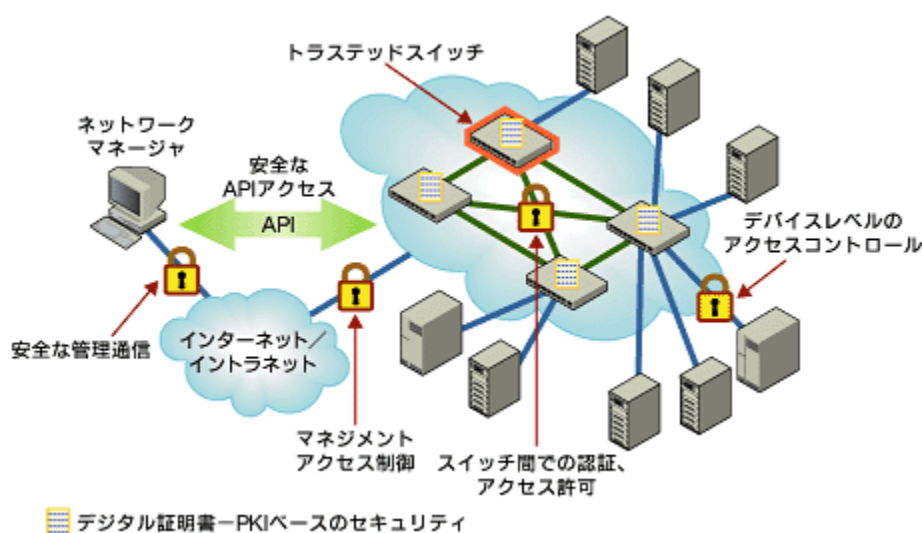


図 7 セキュアな SAN インフラ

また、データ保護という観点でのセキュリティ管理も重要である。データ保護のための SAN インフラとして、WDM 装置や第 2 回で紹介した FCIP (Fibre Channel over IP) ゲートウェイ装置で拠点間の SAN 同士を接続する製品が、ベンダ各社から相次いで登場している。

今回は、ストレージ・ネットワークを拡張するうえで注意すべき事項を解説する予定である。あらかじめ申し上げておくと、ストレージ・ネットワークの拡張においては現在のネットワークの状況を正しく把握しておくことが前提条件である。従って、今回ご紹介した構成管理や変更管理などをぜひ理解したうえで実践するようになりたい。

5. ストレージ・ネットワークの拡張

ストレージ・ネットワーク拡張の背景

初めに、ストレージ・ネットワークを拡張する理由について SAN (Storage Area Network) を例に考えてみよう。SAN を拡張する契機としては、主に以下の 2 つの理由が存在する。

例えばサーバとストレージ間に SAN スイッチ (FC スイッチ) が 1 台だけ存在するような小規模な SAN 構成であっても、多くの場合そこに接続されるデバイスの台数が増えていき、SAN が拡張していく。ここでいう「デバイス」とはサーバとストレージの両方を指すが、筆者が知る限り、特に日本ではサーバ台数の増加によって SAN を拡張することが多い (図 1)。SAN を一度導入すると、ユーザーは概して「共有ストレージをより多くのサーバで使いたい」と思うようになるものだ。共有ストレージはその名の通り、より多くのサーバから使用されるほどその効果を増すわけだから、このような形で SAN が拡張するのは当然だし、また正常な発展であるともいえる。

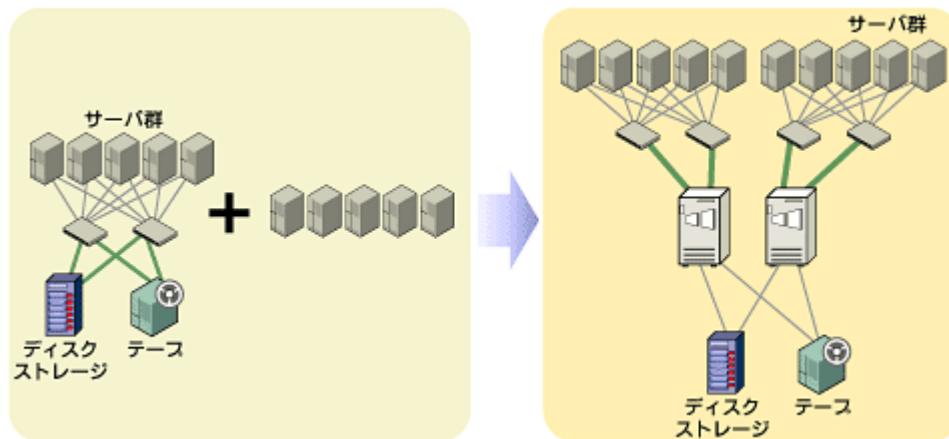


図 1 サーバ台数の増加に伴う SAN の拡張

もう 1 つの理由は、このような小規模な複数の SAN 同士の「統合」である。部門単位あるいはシステム単位で SAN を導入していくと、企業内の各所にこのような「点在化した SAN」が存在することになる。このような SAN を「SAN アイランド」と呼ぶが、多数の SAN アイランドが存在する企業では、ストレージ機器への重複投資が行われているだけでなく、ストレージおよび SAN の管理も重複していることになる。

このような「重複した」機器コストと管理コストは、SAN アイランドの数が増えるほど大きくなり、企業全体で見るとその額は莫大である。従ってこのような管理コストの無駄を抑えるために、SAN アイランド同士を統合することも多い (図 2)。上述のとおり共有ストレージはより多くのサーバから「共有」されるほどその価値を増し、特にテープドライブのようなバックアップストレージではその効果は顕著だ。従って、複数の SAN を統合することにより、パフォーマンスやデータの重要度などに合わせてストレージを使い分け、企業レベルでストレージ資源の全体最適化を実現することが望ましい。

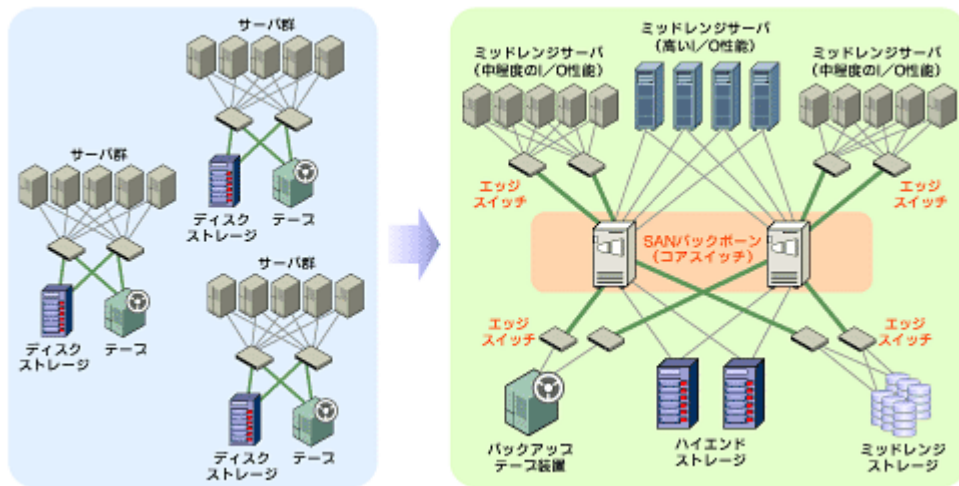


図 2 SAN アイランドの統合

近年はディザスタ・リカバリ(Disaster Recovery:DR)システムのインフラとして SAN を活用するケースも増えている。ディザスタ・リカバリシステムを構築する際には、バックアップデータの一元化と SAN インフラの統合は不可欠な要素だ。なぜなら、バックアップと SAN の一元化が行われていない場合は SAN インフラごとに DR システムが必要となり、いくらコストを掛けてもきりがないからである。

つまり、DR システム導入まで視野に入れて SAN を考えると、

1. 小規模に SAN を導入
2. バックアップを一元化するために、SAN インフラを拡張
3. SAN インフラを DR に活用

という発展形態を見て取れる。DR や BCP(事業継続計画: Business Continuity Plan)を真剣に検討する企業が増えるに従い、WAN 回線の低価格化と広帯域化に歩調を合わせる形で、上記 3 の段階まで SAN インフラを発展させている事例も多くなってきている(図 3)。

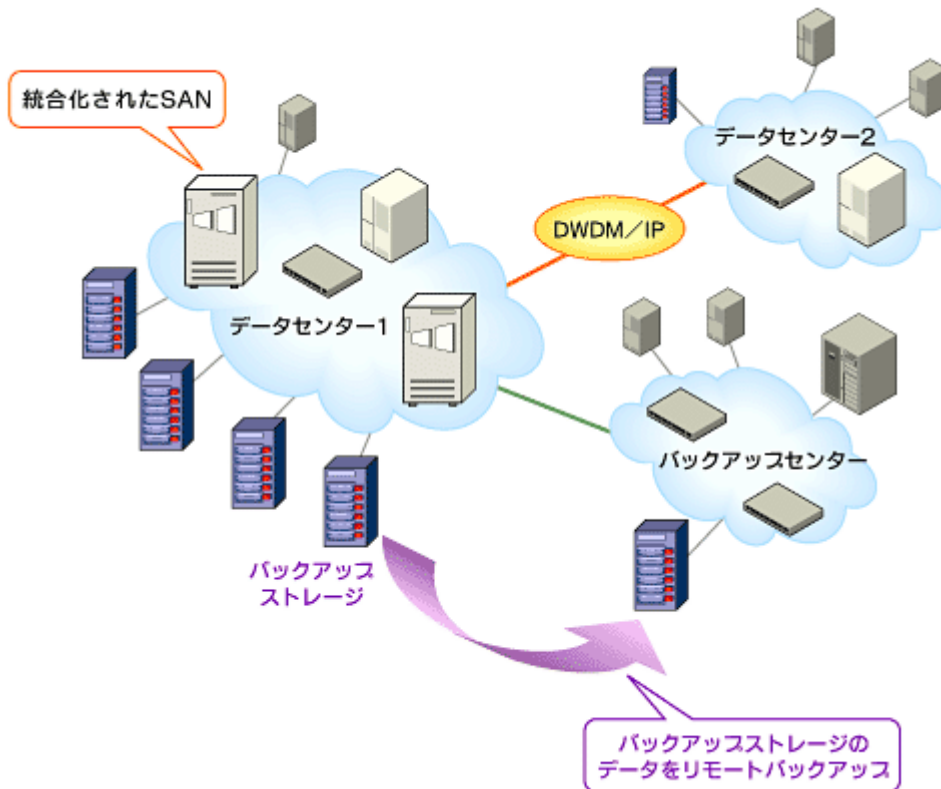


図 3 ディザスタ・リカバリのインフラとしての SAN

さらに「1U サーバ」や「ブレードサーバ」といった、新しくかつ多様なサーバインフラの登場も SAN の拡張に拍車を掛けている。サーバ密度が高いなどメリットが多いことや、近年社会問題化している企業での情報漏えい対策などのため、ブレードサーバ等を利用する企業は増加する一方である。ブレードサーバ(PC)環境ではブレード枚数が飛躍的に増加する。そこで保守性や耐障害性を考慮して OS 領域、アプリケーション領域をすべて外部ストレージに配置し、「SAN ブート」構成を採用することが極めて有効である。この場合、外部／共有ストレージは不可欠の要素となる(図 4)。

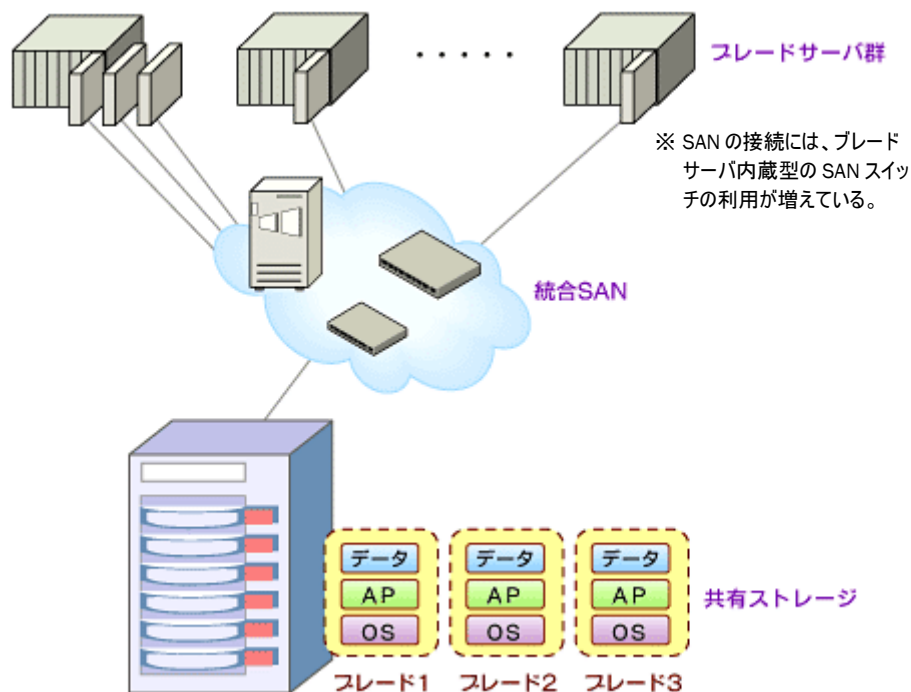


図 4 ブレードサーバと SAN

拡張における手法とそれぞれのメリット・デメリット

では、実際にはどのようにして SAN を拡張すればよいのだろうか。大きく分けると、2つの手法がある。

1つは、図 2 のように既存 SAN 同士をスイッチ間カスケード接続(Inter Switch Link : ISL)して「統合された巨大な SAN」を構築する手法である。この場合、複数スイッチから構成される巨大なファブリックが構成される。この際、サーバおよびストレージを収容する「エッジスイッチ」と、エッジスイッチ間をつなぐ「コアスイッチ」から構成される「コア・エッジ」型のトポロジーで接続し、拡張性に配慮するケースが多い。全体が単一のファブリックとなるため、SAN の一元管理が可能となり、統合後の運用管理コストは低い。しかし、統合に伴って必要となる作業負荷は大きい。例えば複数 SAN を統合して大規模 SAN を構成する場合には、以下の点に注意が必要である。

・スイッチに空きポートが確保されているか

スイッチをカスケード接続する際には、カスケード用のポートが必要になる。つまり、SAN 拡張に伴ってスイッチを増設する場合にはあらかじめ ISL 用ポートを考慮しておく必要があり、すべてのポートを使い果たす前に拡張作業を実施しなければならない。冗長化とパフォーマンス向上のため、ISL は複数本用いるのが一般的である。またスイッチをよりポート数の多いものと交換するようなケースでは、既存スイッチの活用方法についても検討しておくべきだろう。

・それぞれのファブリックのゾーン情報に不整合がないか

それぞれのファブリックでは、デバイスのアクセス制御のためにスイッチで「ゾーニング」を行うのが一般的である。ファブリックを統合する際にそれぞれのファブリック同士のゾーン情報に不整合があると、ファブリック統合が成功しないため、事前に確認しておく必要がある。

・スイッチのドメイン ID に重複がないか

ファブリック内のそれぞれのスイッチには「ドメイン ID」と呼ばれる番号が割り当てられている。この番号はファブリック内で一意である必要があり、ファブリックを統合する前に重複がないかを確認しておく。重複があった場合には、統合前に変更しておかなければならない。

・スイッチのパラメータが一致しているか

FC スイッチではさまざまなパラメータを設定できるが、一部のパラメータはファブリック全体で統一しておく必要がある。これらのパラメータがスイッチ間で一致しない場合、ファブリック統合が失敗するため、こちらも統合前に確認のうえ、必要に応じて変更しておく。

・接続構成が変更しても、サーバ OS がストレージを問題なく認識できるか

スイッチの構成変更に伴ってドメイン ID が変更されるケースなどでは、サーバの HBA や OS によっては、ストレージデバイスを再認識させるための設定が必要となる場合がある。サーバ停止を伴うことになるため、事前確認が欠かせない。

上記の注意点は、使用しているスイッチやサーバ OS、ストレージ装置などにより違いがあるが、いずれにしても事前に調査しておくべき事項だ。

もう 1 つの手法は、ファブリック同士を「SAN ルータ」と呼ばれる機器で接続し、ファブリックを統合することなく、必要なデバイスのみを共有するものである。例えばバックアップ用のテープライブラリを、ほかのファブリックからアクセス可能にするといった使い方ができる。SAN ルータによって、それぞれのファブリックは一種の「サブネット」のように位置付けられる。各ファブリックは物理的には SAN ルータ経由で接続（結線）されているが、論理的には独立して存在している。つまり、ファブリック内のルーティングアルゴリズムである FSPF (Fabric Shortest Path First) の計算処理や、ファブリック内で機器の状態変更を通知する RSCN (Registered State Change Notification) といったファブリックイベントは、SAN ルータを超えては伝播しない。また、それぞれのファブリックにおいてゾーン情報やネームサーバ情報を保持することになる。このようにファブリック同士を SAN ルータで接続した巨大な SAN インフラを、当社では「メタ SAN」(Meta SAN)と呼んでいる(図 5)。

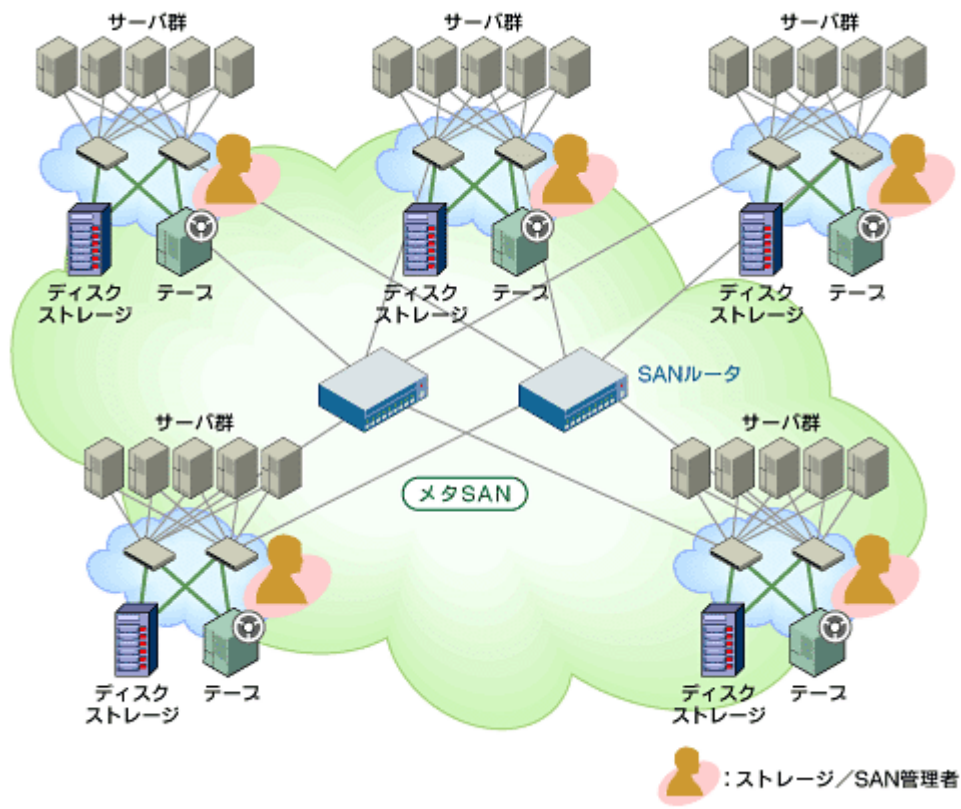


図5 SAN ルータによるメタ SAN の構成

メタ SAN 内のファブリックは統合されていないため、すでに接続されている機器に対する影響はない。従って、上記で説明したようなファブリック統合時の注意点に関しても、SAN ルータ接続環境では考慮しなくてよいため、より簡単に実現できる方法である。しかしファブリックは独立して存在し続けているため、個々のファブリック単位で引き続き管理を行う必要がある。「管理負荷を少なくする」という観点では、SAN 統合に比べてメリットはない。

最終回となる次回は、「ストレージ・ネットワークはどこへ向かうのか？」と題し、今後この分野で登場してくると思われる、さまざまな技術を紹介していく。

6. ストレージ・ネットワークはどこへ向かうのか

ストレージ・ネットワークにかかわる最新技術の可能性と注意点

最終回のタイトルを仰々しくも「ストレージ・ネットワークはどこへ向かうのか」としたが、データアクセスのインフラとしてのストレージ・ネットワークに求められる役割は、今後ますます大きくなっていくと考えられる。サーバとストレージ、さらにはクライアントがつながるストレージ・ネットワークは、「サーバ管理の効率化」「ストレージ管理の効率化」「クライアントアクセスの効率化」といった機能を包含し、より「インテリジェント」なものになっていくだろう(図 1)。本稿では、「新しいネットワーク・インフラ」「ストレージ仮想化」「サーバ仮想化」「ファイルアクセス技術」「ILMとFLM」という4つの技術に関して、それぞれのメリットと検討および導入における注意点を解説する。

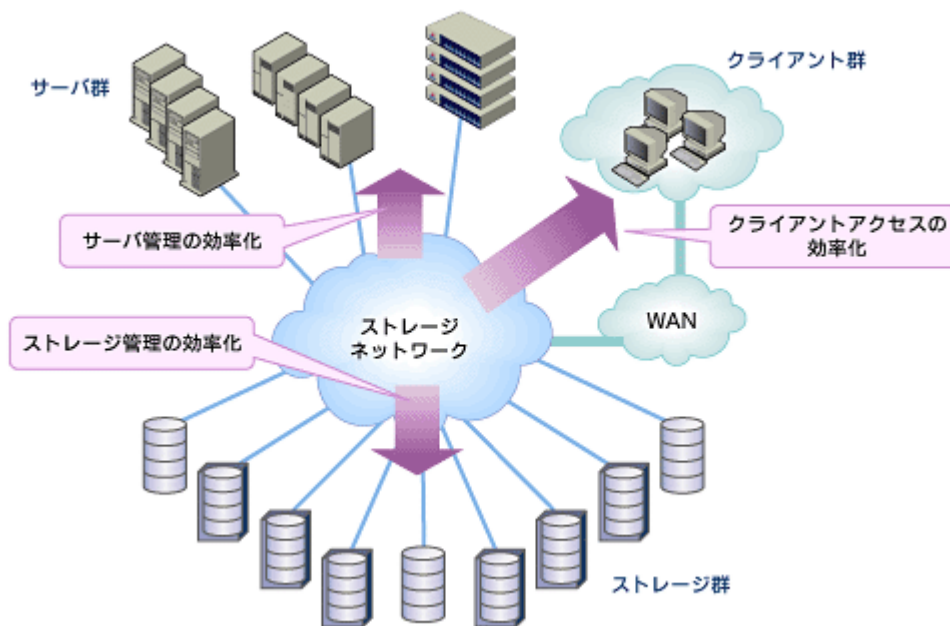


図 1 ストレージ・ネットワークの進化

新しいネットワーク・インフラ

ストレージ・ネットワークを構成するインフラに関わる技術は日進月歩で発展している。前述した 8Gbps ファイバチャネル以外にも、SAN のレベルで仮想ホスト単位の QoS (Quality of Services)を実現する機能、ストレージ内のデータ移動やデータの暗号化を行う機能など、ネットワーク・インフラがますます高度化してきている。

プロトコルが多様化していくことも、注目に値する。現在 SAN で使用されるプロトコルはファイバチャネルもしくは iSCSI であるが、現在大手ベンダを中心に規格化が進んでいるのが、「FCoE (Fibre Channel over Ethernet)」だ(図2)。元々ファイバチャネルとイーサネットはお互い影響は受けあっているものの、物理層レベルからそれぞれが独立して規格化されているため、基本的に両者に互換性はない。FCoE はファイバチャネルの通信をイーサネットフレーム上で行うことを可能にする技術であり、ファイバチャネルとイーサネットを融合するものだ。ただ、イーサネットはファイバチャネルが提供するようなフロー制御や輻輳制御などの仕組みを標準では持っていないため、ファイバチャネル、ひいてはさらにその上位で SCSI プロトコルが稼動するインフラとしてのイーサネットには、既存のイーサネットを拡張する技術が必要になる。このように拡張されたイーサネットは「CEE (Converged Enhanced Ethernet)」と呼ばれ、10Gbps 以上の速度を前提とし、FCoE が動作するイーサネットも CEE である。また、ファイバチャネルを直接イーサネットフレーム上で動作させるのも FCoE の特徴である。TCP/IP を使用しないために通信におけるオーバーヘッドが少なく、ストレージ I/O に向くプロトコルであるといえる。

Application	Applications				
SCSI	SCSI				
Encapsulation	iSCSI	FC	FC	FC	SRP
	TCP	FCIP	iFCP		
		TCP	TCP		
IP	IP	IP	FCoE		
Transport	Ethernet				Infiniband

↑ iSCSI
↑ FCIP
↑ iFCP
↑ FCoE
↑ IB

※FCoE は、現在規格化が進められている新しいプロトコル。トランスポートレイヤには FCoE 用に拡張された 10Gbps の Ethernet が必要。

図2 FCoE (Fibre Channel over Ethernet)

ストレージ仮想化

ストレージ仮想化は以前より注目されていた技術で、すでに多くのベンダから製品が提供されている。ストレージを仮想化することで、ユーザーは物理的なストレージを意識することなく、柔軟に複数のストレージを管理できる。例えば、複数の物理ストレージから構成される「仮想ボリューム」を作成して自由に容量を追加したり、サーバに意識させずにストレージ装置間でデータ移動を実施することなどができる(図3)。

ストレージ仮想化を実現するには、いくつかの形態がある(図4)。1つは専用のアプライアンス装置やソフトウェアを利用するものだ。以前から提供されていた形態で、現在最も普及しているといえる実装方法だろう。この場合すべての I/O がアプライアンス装置もしくはソフトウェアを通過するため、パフォーマンス上のボトルネックになる懸念がある。特にソフトウェア製品として提供されているものについては、動作環境のハードウェアを十分に注意して選定するこ

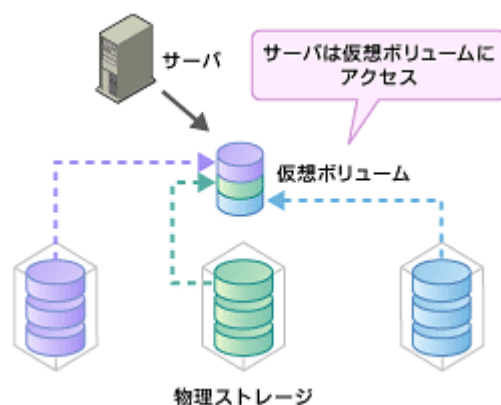


図3 ストレージの仮想化

とが望まれる。

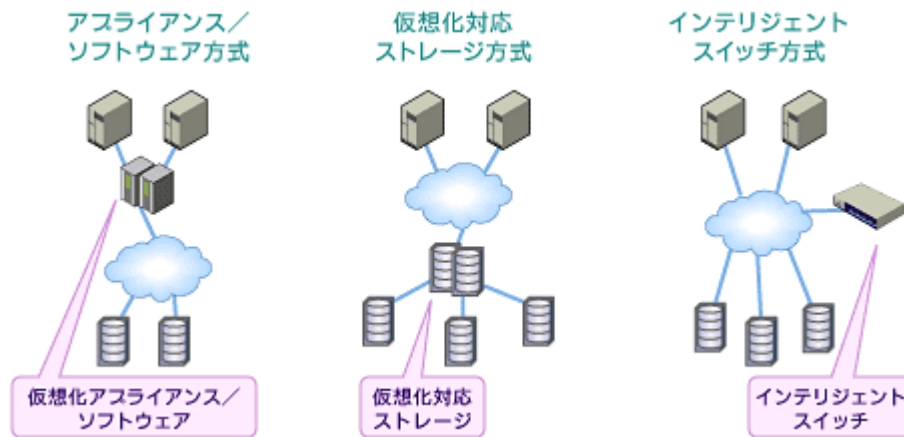


図4 ストレージ仮想化を実現する各種の形態

2つ目は「ストレージを仮想化するストレージ」を用いる方式である。仮想化ストレージの配下に複数の物理ストレージを移し、仮想化ストレージ以外のストレージをサーバから隠す形態だ。ハードウェアベースであるため十分なパフォーマンスを発揮できるが、実現できる機能やサポートされる物理ストレージは仮想化ストレージに依存する。また、そもそもストレージ仮想化のメリットの1つは特定の物理ストレージベンダ依存から脱却することだが、ストレージベースでの仮想化ではやはり仮想化ストレージを提供するベンダに依存することになる。

近年注目を集めているのが、「インテリジェントスイッチ」を導入してストレージを仮想化する方式である。ストレージ仮想化に対応した SAN スイッチを専用の端末から制御する。これらの間のインターフェイスは、ANSI T11.5 委員会で「FAIS (Fabric Application Interface Specification)」として標準化されている。この形態ではデータ I/O と制御用の I/O が分離して処理されるため、高負荷時にもパフォーマンスのボトルネックが発生しにくい。しかし現時点ではまだ市場での実績が多いとはいえ、導入に際しての十分な事前検証が欠かせない。

上記のいずれの方式で仮想化を実現するにしても、障害時の切り分けはこれまでよりも困難になる。例えばインテリジェントスイッチで仮想化を行っている場合には、「障害が発生しているのがストレージ側なのかスイッチ側なのか」「ハードウェア障害なのかソフトウェア障害なのか」など、単純にサーバを物理ストレージに接続する場合に比べて考慮しなければならない点が増える。従って運用上のメリットばかりに注目するのではなく、導入する製品の物理的あるいは論理的な仕組みについてもきちんと理解しておかなければならない。

サーバ仮想化

ストレージ・ネットワークにはストレージだけではなく、「サーバ」も接続されている。ストレージ・ネットワークの規模が大きくなるにつれて接続されるサーバ台数も増加するため、「増え続けるサーバ」への対処も管理者にとっては頭の痛い問題だ。

サーバ仮想化について理解するには、まず「サーバ」の定義をあらためて見直す必要がある。一般に物理的なサーバには、「CPU」「メモリ」「NIC(Network Interface Card)」「ディスクドライブ」「OS」「アプリケーション」などのコンポーネントが含まれている。1 台の物理サーバには、上記のコンポーネントが1 つもしくはそれ以上存在するのが一般的だ。つまり、これまでの物理サーバ環境では、「サーバ(物理サーバ)」と「コンポーネント」の関係は 1:1 もしくは 1:n であった。しかし「仮想化された」サーバ環境では、この関係が n:1 になり得る。例えば、複数の(仮想)サーバで1 つの物理 CPU や NIC を共有するといった使い方が可能になる(図5)。

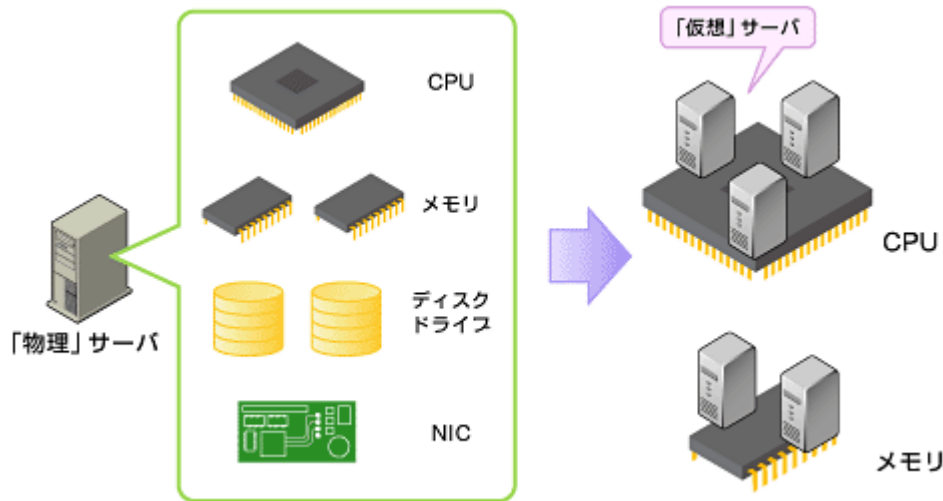


図5 サーバの仮想化

仮想サーバ環境では、「サーバ」は物理的なコンポーネントから独立したものと認識される。つまりCPUやメモリ、HDDといった物理リソースをその用途や求められるパフォーマンス、可用性などに応じて柔軟に組み合わせ、仮想サーバを動的に構成することが可能となる。従って、仮想サーバ環境を構築する場合には、それぞれの物理コンポーネントは「切り離されている」方が実装しやすい。例えばストレージ・ネットワークを中心にしてディスクドライブには外部ストレージを利用し、OSやアプリケーションは外部ストレージ上にインストールしておけば、コンピューティングリソースとしてのCPUおよびメモリと組み合わせ、自由に仮想サーバをインスタンス化することができる(図6)。

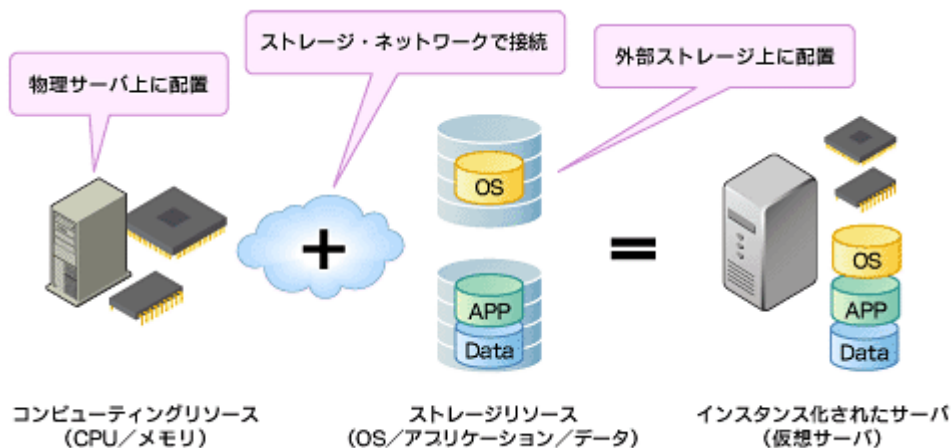


図6 リソースを柔軟に組み合わせて論理的なサーバを構築

システム拡張やハードウェア障害などにより物理サーバを交換するような場合には、サーバを動的に構成できるメリットは運用保守の観点からは非常に大きい。従って、前回紹介したブレードサーバを用いたシステムなどでは、サーバの仮想化技術は検討に値する選択肢になるだろう。

新しいファイルアクセス関連技術

本連載の第2回でファイルアクセスとブロックアクセスについて説明したが、私たちは「ファイル」という単位で日常的にデータに接している。企業内のあらゆる情報がファイルという形で保存され、その数とデータ容量は増加する一方だ。企業が保有しているデータの約4分の3は支店や営業所のファイルサーバに格納されているともいわれており、企業レベルでのデータ管理を考えるうえでもファイルの効果的な管理が求められる。

多くの企業で拠点に分散するファイルサーバの統合が課題になっているが、その際に問題となるのが「ファイルアクセスのパフォーマンス」と「アクセスパス」である。ファイルサーバを本社などのデータセンターに統合した場合、拠点のクライアントは WAN 経由でファイルサーバにアクセスすることになる。CIFS(Common Internet File System)や NFS (Network File System)といったファイルサーバへのアクセスに標準で利用されるプロトコルはクライアントとサーバ間でのデータのやりとりが非常に多く、WAN 環境ではパフォーマンス上問題になることが多い。またファイルサーバが変更されるため、拠点のクライアントは新しいファイルサーバ名とフォルダへのアクセスパスを設定し直す必要がある。クライアント PC 上にショートカットを作成している場合にはそれらをすべて変更しなければならず、変更に伴う手間は非常に大きい。

上記の問題を解決する手段として、「WAN 高速化装置」と「グローバルネームスペース」という技術を実装した製品がベンダ各社から提供されている。WAN 高速化装置は WAN 経由でのファイルアクセスを高速化する技術だ。WAN 高速化装置同士は専用のプロトコルで通信しており、CIFS や NFS を使用する場合に比べてパフォーマンスは大幅に向上する。

グローバルネームスペースは、DNS(Domain Name System)のようにクライアントからファイルサーバへのパス (Windows であれば UNC パス)と、対応するファイルサーバの関係を管理し、クライアントからのアクセスを一元化する(図 7)。

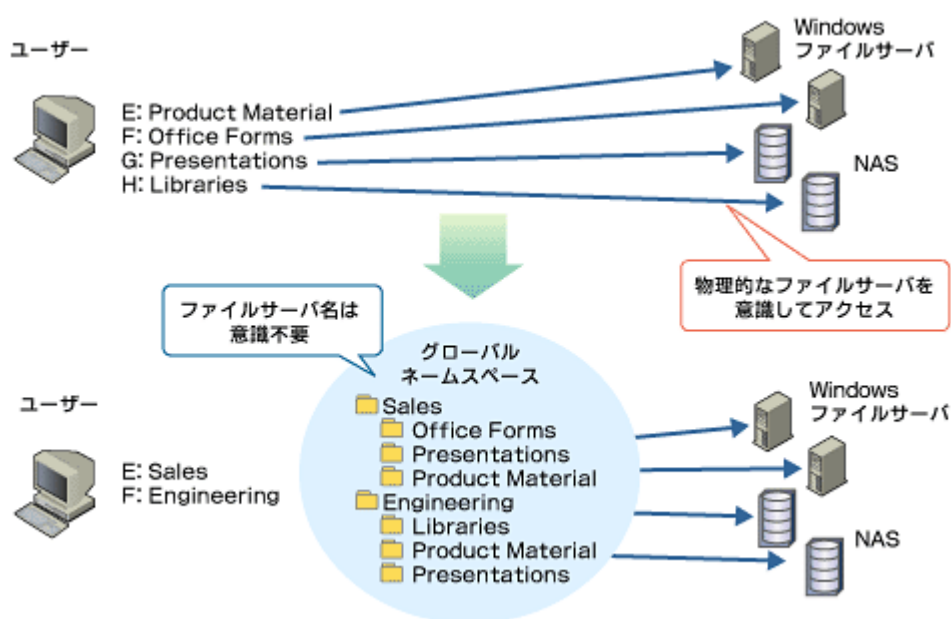


図 7 グローバルネームスペースによるファイル利用環境の統合

例えば私たちが www.brocade.com の IP アドレスを知らなくても [brocade.com](http://www.brocade.com) の Web サーバにアクセスできるのと同じように、グローバルネームスペースを使えば物理的なファイルサーバを認識する必要はなくなる。ファイルサーバを統合したり変更したりした際に、ファイルサーバへのアクセスパスが変わるケースは多い。グローバルネームスペースはそのような場合に特に有効な技術だ。ただ、現在グローバルネームスペースを導入しているユーザー企業はまだそれほど多くない。導入実績が増えてくるのはこれからである。

ILM と FLM

効果的にデータを管理するには、その「ライフサイクル」にも注目すべきだ。すべてのデータが、常に頻繁にアクセスされるわけではない。一般にデータは作成された直後は頻繁にアクセスされるが、時間の経過とともにアクセス頻度は低くなる。またデータの重要度も、高いものもあればそうでないものもありさまざまだ。従って、データのアクセス頻度や重要度を無視してすべてのデータを高機能・高価格のストレージ装置に格納しておくのは、データ格納やバックアップに伴うコストを考えると最適とはいえない。そこで、データの重要度とアクセス頻度に合わせて最適なストレージを使い分ける、つまりストレージを階層的に利用することを目指して登場した概念が ILM(Information Lifecycle Management)である(図 8)。

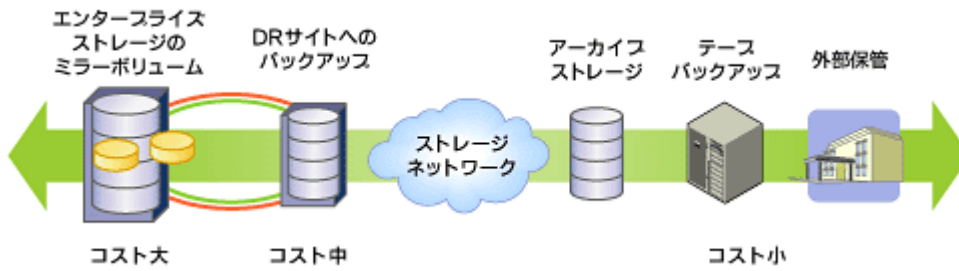


図 8 ILM の考え方

FLM (File Lifecycle Management)とは、ILM の考え方をファイルサーバに対応させたものだ。ファイルサーバにも高価なものもあれば低コストのものもある。また、ファイルサーバのデータバックアップは日常の運用業務の中でも特に負荷の大きいものである。そこでファイルについてもライフサイクルに合わせたポリシーを定義し、そのポリシーに見合ったファイルサーバにデータを格納すれば、最適なコストでファイルを管理することが可能になる。

本連載は今回で終了である。これまでの計 6 回の連載の中でストレージ・ネットワークが果たす役割や、それといかに上手に付き合うべきか、ということ筆者なりの視点で説明してきたつもりである。本連載の内容が今後のストレージ・インフラ管理のお役に立てば、何よりの喜びである。