2.4 ストレージネットワーキング

午後試験では，サーバ間でストレージを共有する事例や，広域災害に備えて遠隔地のバックアップサイトにリモートバックアップを行う事例がしばしば登場する。その中で，ストレージネットワーキングの基礎的な知識が問われる場合がある。過去には設計の応用問題が出題されたこともあったが，本文中に動作原理が詳しく説明されており，基礎知識から推論できるように配慮されていた。したがって，基礎知識をしっかり学習しておくことが大切である。

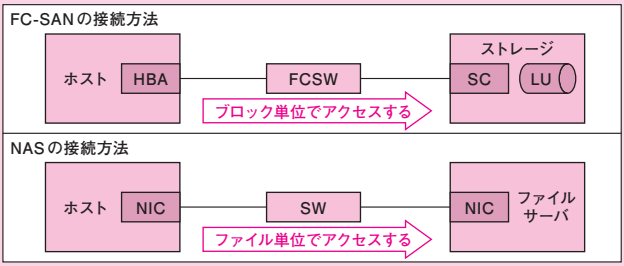
2.4.1 SAN と NAS

複数のサーバ間で，ネットワークを介した磁気ディスク装置の共有を可能にする技術として，**SAN**（Storage Area Network），**NAS**（Network Attached Storage）がある。

SAN のストレージデバイスは，サーバに直接接続された SCSI（Small Computer System Interface）のストレージデバイス（raw デバイス）と機能的に同等である。ホストとロジカルユニット間のデータのやり取りには SCSI コマンドを使用し，**ブロック単位**でアクセスしている。

NAS は，ファイルサーバと機能的に同等である。ネットワーク上のストレージに対し，ファイル共有プロトコルを使用し，**ファイル単位**でアクセスしている。

両者のアクセス方法を次の図に示す。



図：SAN と NAS のアクセス方法

試験に出る

SAN と NAS の比較について，平成 23 年午前Ⅱ問 7 で出題された

なお，この図に登場するSANは，SANの一種である**FC-SAN**である（FC-SANについては後述する）。

ホストとSANのストレージは，**ファイバチャネルスイッチ**（以下，FCSWと称する）を介して接続している。ホストのインタフェースは**ホストバスアダプタ**（以下，HBAと称する）である。ストレージのインタフェースは，**ストレージコントローラ**（以下，SCと称する）である。

SANのストレージには，物理ディスク装置が何台も搭載されている。RAIDコントローラにより物理ディスクを束ねた上で，各ホストが必要とする容量に基づき，全体を幾つかに区分する。区分された個々の領域が，外部に提供する論理的なディスクとなる。この論理なディスクを**ロジカルユニット**（以下，LUと称する）と呼ぶ。

このLUに対し，ホストはSCSIコマンドを使用してブロック単位でアクセスする。

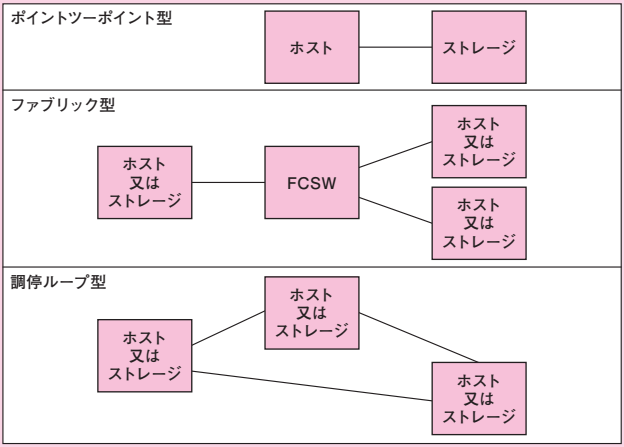
一方，ホストとNASは，通常のスイッチ（以下，SWと称する）を介して接続している。NASはファイルサーバと同等であるので，ホストとNASはIPアドレスをもっている。

●ファイバチャネル

ファイバチャネル（FC：Fibre Channel）は，ANSIのT11で標準化された，高速かつ高信頼性を特徴とするデータ転送の規格である。

FCの接続形態には，ポイントツーポイント型（Point to Point），**ファブリック**型（Fabric），調停ループ型（Arbitrated Loop）の3種類があるが，SANで一般的に用いられているのは，ファブリック型である。

ファブリック型は，1台のスイッチに対し，1台以上のホスト又はストレージが接続される構成である。スイッチ同士を接続することもできる。



図：FC のトポロジ

●WWN とポートアドレス

WWN（World Wide Name）とは，FC のノード対して，全世界で一意に割り当てられた番号である。ここで言う「ノード」とは，ホストの HBA，FCSW，ストレージの FC インタフェースなどを指す。WWN は，ちょうどイーサネットの MAC アドレスに似ている。

HBA や FCSW のポートには，ポートアドレスが動的に割り当てられる。

●ゾーニング

FCSW に接続するサーバやストレージを複数のグループに分けることができる。このグループのことを**ゾーン**という。1台のスイッチに複数のゾーンを定義する機能のことを，**ゾーニング**という。

異なるゾーンに所属する機器（サーバ，ストレージ）は，互いに通信することができない。ゾーンの定義はポート単位又は WWN 単位で行う。1 個のポートを複数のゾーンに所属させることができる。

試験に出る

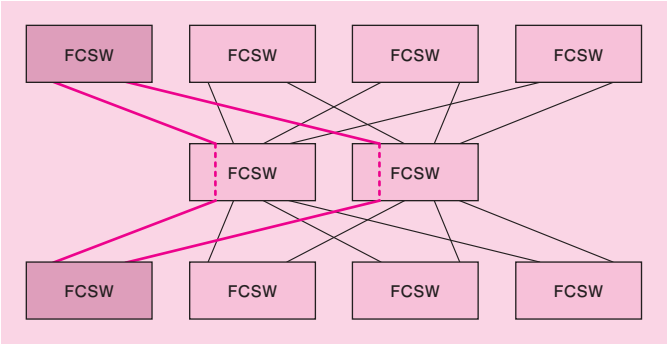
FSPFについて，平成23年午後Ⅱ問1で出題された。ホストとLU間の経路の冗長化について，平成24年午後Ⅱ問1で出題された

●FCの冗長構成

スイッチ間の経路を複数持たせ，冗長構成にすることもできる。FCが規定している経路制御方式である**FSPF**（Fabric Shortest Path First）は，FCSWのホップ数をコストとして評価し，SPF（Shortest Path First）アルゴリズムに基づいて最小コストの経路を決定する仕組みになっている。

コストが等しい経路が複数あるとき，それら経路を同時に使用できる。

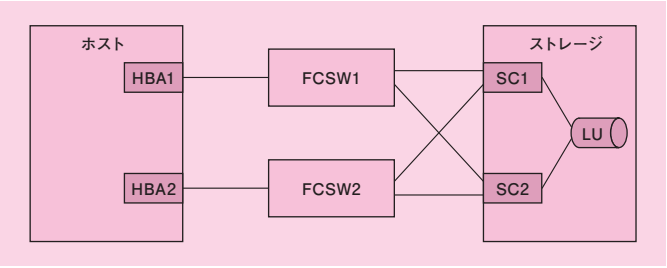
冗長構成を採ったファブリックの例を次の図に示す。左上のFCSWと左下のFCSW間の経路は二つあり（図中の赤線），どちらもコストが等しいので，同時に使用される。



図：冗長構成を採ったファブリックの例

ホストとLU間の経路を冗長化するときは，ホストのHBA，FCSW，ストレージのSCをそれぞれ冗長化する。例えば，次の図では，ホストとLU間の経路は四つある。

経路①：ホスト→HBA1→FCSW1→SC1→LU
経路②：ホスト→HBA1→FCSW1→SC2→LU
経路③：ホスト→HBA2→FCSW2→SC1→LU
経路④：ホスト→HBA2→FCSW2→SC2→LU



図：ホストと LU 間の経路を冗長化した例

●FC-SAN と IP-SAN

SAN は，FC-SAN と IP-SAN に大別される。

FC-SAN は，FCSW によって構成される，ストレージ共有のためのネットワークである。

IP-SAN は，FC フレーム又は SCSI フレームを TCP/IP にカプセル化し，IP ネットワーク上に SAN を構築するものである。

IP-SAN について，詳しくは本章の「2.3.2　SAN のプロトコル」で解説する。

●拡張イーサネット（統合ネットワーク）

拡張イーサネットとは，IEEE802.1 委員会の DCB タスクグループで規格化されている **DCB**（Data Center Bridging）のことである。

伝送速度は 10Gbps であるが，従来のイーサネットをただ単に広帯域化したものではない。これは，FC-SAN（Fibre Channel Storage Area Network）を伝送することを目的として，イーサネットの機能を拡張し，FC が有していた高信頼性（ロスレス）などの優れた特性にできる限り近づけたものである。

拡張イーサネットでは，**CNA**（Converged Network Adapter）と呼ばれるネットワーク接続アダプタを使用する。これは，1 個のアダプタで HBA と NIC を兼ね備える機能をもつ。

今日，IP ネットワークはイーサネット上に構築されている。したがって，高信頼性を有する拡張イーサネットを構築すれば，FC-SAN と IP ネットワークを統合することができる。そのメリットは多々ある。まずは，IP ネットワークの側からすれば，レイヤ 2 の機能拡張がもたらす高信頼性を享受できる。ネットワーク全

拡張イーサネット（SAN と LAN の統合）について，平成 24 年午後Ⅱ問 1，平成 23 年午後Ⅱ問 1 で出題された

体からすれば，ネットワークの統合によるケーブリングの簡素化，省電力化，運用負荷の軽減などが期待できる。

拡張イーサネットについて，詳しくは本章の「2.3.2　SAN のプロトコル」で解説する。

2.4.2 SAN のプロトコル

用語解説

ロスレス
損失がないこと。ストレージトラフィックにおいては，特に，パケットロスがないことをいう

ここでは，FC-SAN，IP-SAN，拡張イーサネットのプロトコルについて解説する。

ストレージトラフィックでは，高信頼性（**ロスレス**）が求められている。高品質の光ファイバを伝送路として使用すれば，伝送路上でのビット誤りはまず発生しない。それゆえ，パケットロスの要因は，通常，**バッファの枯渇**である。

バッファの枯渇を防ぐには，適切な**フロー制御**が欠かせない。そこで，各プロトコルのフロー制御についても解説する。

●FC-SAN

FC のプロトコルスタックは，次に示す階層構造をしている。

表：FC のプロトコルスタック

階層	内容
FC-4 層	上位プロトコルとのマッピングを規定する（上位プロトコルのカプセル化に加え，上位層プロトコルの伝送手順を FC の下位層の該当するものに割り当てる場合がある）
FC-3 層	暗号化機能などを規定する（規定されているが，実装している製品は存在しない）
FC-2 層	フロー制御，伝送手順などを規定する
FC-1 層	8B/10B と呼ばれる符号化方式，パラレル／シリアル変換を規定する
FC-0 層	コネクタ，ケーブル，伝送メディアなどの物理的インタフェースを規定する

SCSI は，FC の上位プロトコルに位置する。SCSI をカプセル化した FC-4 層のプロトコルは，FCP である。それゆえ，FC-SAN では FCP が用いられている。

●FC-SAN のフロー制御

FC-SAN のフロー制御は，TCP のそれと比較すると理解しやすい。「相手が受信できるだけのフレームしか送信しない」という

点で，TCP とよく似ているからだ。

具体的に言うと，FC-SAN のフロー制御は，次のような仕組みになっている。

- **準備**
  通信を開始する前に，隣接するノード間で，自分の空きバッファ数を相手に通知しておく。相手側の空きバッファ数のことを「**クレジット**」という。
  FC-SAN は，クレジットを管理しながらフロー制御を行っている。

- **送信と受信**
  1. 相手に 1 フレーム送信したら，クレジットを 1 つ減らす。
  2. 相手から応答が返ってきたらクレジットを 1 つ増やす。

- **連続転送**
  FC-SAN では，クレジットが 0 になるまでは複数のフレームを連続転送することができる。クレジットが 0 になったら，相手から応答が返ってくるまで，フレームを送信しない。

FC-SAN の「クレジット」を TCP の「ウィンドウサイズ」に読み替えれば，FC-SAN と TCP/IP のフロー制御は，似ていることが分かるだろう。

しかし，両者には大きな相違点がある。

それは，「準備」のところで触れたとおり，FC-SAN では，「隣接するノード間」でフロー制御を行っている点だ。

つまり，TCP/IP のフロー制御が **End-to-End** で制御されるのに対し，FC-SAN では **Buffer-to-Buffer** で制御されているのである。

TCP/IP の場合，経路途中のどこかのノードでバッファ枯渇が発生したとしても，エンドシステムは（少なくともウィンドウサイズからは）そのことを知ることができない。したがって，ウィンドウサイズが 0 でなければ，相手のバッファ容量には余裕があると判断し，パケットを送信する。その結果，バッファ枯渇が発生したその場所で，パケットがロスしてしまうことになる。

一方，FC-SAN の場合，Buffer-to-Buffer であるため，隣接ノー

ド間の局所的なバッファ枯渇に対処できる。

前述のとおり，FC-SAN のフロー制御は，バッファの容量を相互に逐次確認し合うことで，相手のバッファが枯渇しないように，相手の状況に応じてフレームを送信している。FC-SAN は，通信経路上のあらゆる隣接ノード間で，このバッファ管理に基づくフロー制御を実施している。

したがって，各ノードのバッファが枯渇せず，枯渇に起因するフレームのロスを防止することができる。

試験に出る

FC-SANのフロー制御について，平成 23 年午後Ⅱ問 1 で出題された

●IP-SAN

IP-SAN の通信規格には，**iSCSI**（Internet SCSI），iFCP（Internet Fibre Channel Protocol），FCIP（Fibre Channel over IP）がある。

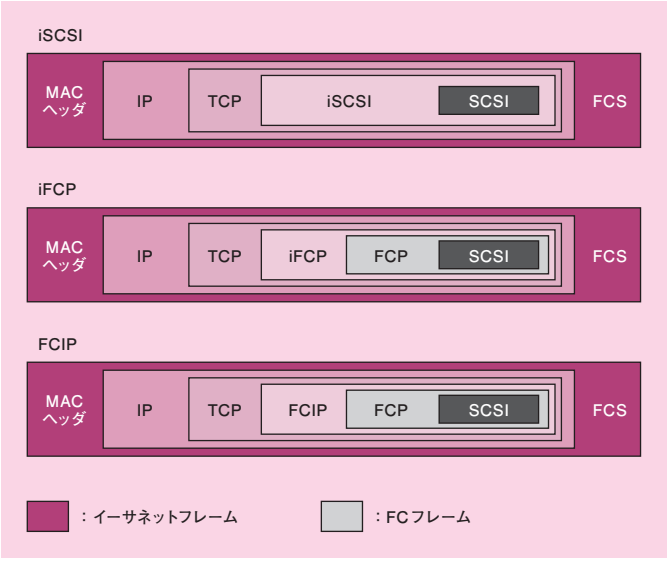
iSCSI は SCSI コマンドを TCP/IP パケットにカプセル化しており，FC デバイスを用いることなく，IP ネットワークだけで構成する。

これに対し，iFCP，FCIP は，FC-SAN の通信で用いられている FC フレームを TCP/IP パケットにカプセル化している。

これら三つのプロトコルのプロトコルスタックを次の図に示す。

試験に出る

IP-SAN について，平成 23 年午後Ⅱ問 1，平成 22 午後Ⅱ問 1 で出題された。iSCSI のイニシエータやターミネータについて，平成 22 年午後Ⅱ問 1 で出題された



図：IP-SAN のプロトコルスタック

- **iSCSI**

  iSCSI は，iSCSI 対応のストレージを用意するだけで，既設の IP ネットワーク環境に共有ストレージ環境を構築できる。その導入容易性から，IP-SAN の中で最もよく用いられている。

  iSCSI は，イニシエータからターゲットに SCSI コマンドを発行することによって，サーバとストレージ装置間でブロックデータの入出力が実現される仕組みになっている。

  イニシエータとは，サーバで稼働し，SCSI コマンドを発行するソフトウェアである。**ターゲット**とは，ストレージ装置で稼働し，SCSI コマンドの処理を実行するソフトウェアである。

  なお，イニシエータソフトウェアをサーバにインストールする代わりに，iSCSI のプロトコル処理をハードウェアで実行する iSCSI HBA をサーバに搭載してもよい。

- **iFCP と FCIP**

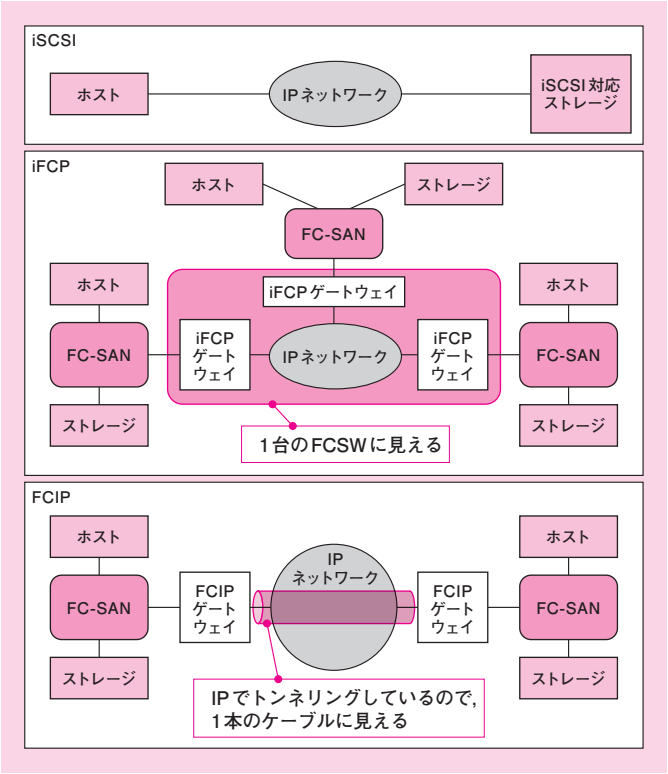
  iFCP と FCIP は，プロトコルスタックだけなら，どちらも同じように見える。事実，両者とも FCSW 間を IP ネットワークで接続し，あたかも FC-SAN の伝送距離を延長しているような構成になっている。

  とはいえ，iFCP と FCIP は，FC から IP ネットワークがどのように見えるかが異なっている。これが，両者の接続方式に相違をもたらしている。

  iFCP からは，IP ネットワークがあたかも 1 台の FCSW のように見える。したがって，IP ネットワークに対し，3 拠点以上の FC-SAN を接続することができる。

  一方，FCIP からは，IP ネットワークがあたかも 1 本のケーブルのように見える。なぜなら，FC フレームを IP でトンネリングして転送しているからだ。したがって，IP ネットワークに対し，2 拠点の FC-SAN だけを接続することができる。

  比較のために，iSCSI，iFCP，FCIP の接続方式を次の図に示す。



図：IP-SAN の接続方式

●IP-SAN のフロー制御

iSCSI は，TCP/IP のフロー制御を行っている。

iFCP，FCIP は，IP ネットワーク上の伝送では TCP/IP のフロー制御を行っている。

●拡張イーサネット（統合ネットワーク）

FC-SAN と統合ネットワークをフレームフォーマットで比較してみると，「統合」のイメージをつかみやすくなる。

- **FC から見た下位層**

  FC フレームは，FC-SAN によって伝送されている。

  一方，統合ネットワークでは，FC フレームを **FCoE**（Fibre Channel over Ethernet）フレームでカプセル化し，この

FCoE フレームを拡張イーサネットフレームがカプセル化している。そして，拡張イーサネットフレームは，統合ネットワークによって伝送されている。

したがって，FCoE のカプセル化の仕組みにより，FC の観点からは，FC-SAN と統合ネットワークは，自分を伝送する媒体（物理層）に見える。

もちろん，これはあくまでフレームフォーマット上の話である。伝送媒体を FC-SAN から統合ネットワークに置き換えるには，同等の伝送品質を提供できなければならないので，従来のイーサネットからの機能拡張が必要となったわけだ。

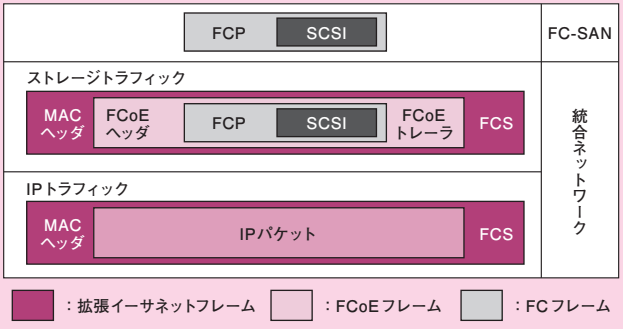
- **拡張イーサネットから見た上位層**

拡張イーサネットフレームのフォーマットは，通常のイーサネットの **VLAN フレーム**と同じである。FCoE フレームと IP パケットは，イーサネットフレームのタイプ値が異なるだけである。イーサネットの観点からは，どちらも上位層に見える。

したがって，フレームフォーマット上は，ストレージトラフィックと IP トラフィックを統合できていることになる。

詳説

拡張イーサネットフレームの VLAN タグには，トラフィックの優先度が格納される。優先度について，詳しくはすぐ後の「● 統合ネットワークのフロー制御」を参照していただきたい

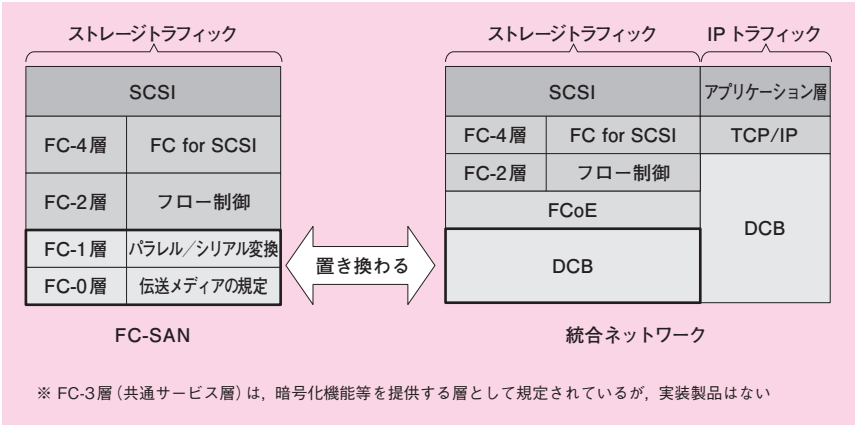


厳密に言うと，FC フレームの前後には，SOF（Start Of Frame）と EOF（End Of Frame）が付与される。FCoE ヘッダは FC の SOF を，FCoE トレーラは FC の EOF を，それぞれ格納している（SOF，EOF のコード値を変換した上で，格納している）。

図：フレームフォーマットの比較

FC-SAN の階層を統合ネットワークのプロトコルスタックに当てはめてみると，次の図「プロトコルスタックの比較」となる。

ただし，この比較は，厳密なものではない。



図：プロトコルスタックの比較

簡単に言うと，拡張イーサネットは，FC の FC-0 層～ FC-1 層に置き換わっている。

FC-SAN は，SCSI を使用した raw デバイスへのアクセスをネットワーク経由で提供している。FC は，ストレージに送受信する SCSI コマンドやデータを FC フレームにカプセル化する機能を有する。SCSI はパケットロスを前提としないプロトコルなので，SCSI の下位層が信頼性を確保する必要がある。まさしく FC はその信頼性を提供しており，フロー制御など，高信頼性を確保する機能が実装されている。

IP ネットワークとの統合を果たすには，FC-0 層～ FC-1 層をイーサネットに置き換える必要がある。しかし，FC-SAN と統合するには，イーサネットは信頼性の点で劣っている。そこで拡張イーサネットが必要になったわけだ。

●統合ネットワークのフロー制御

前述のとおり，FC-SAN の FC-0 層～ FC-1 層が，拡張イーサネットに置き換わる。

ストレージトラフィックの場合，上位層は FC-2 層～ FC-4 層と

なる。前述の「クレジット」を用いたフロー制御は FC-2 層なので，拡張イーサネットには，上位層の信頼性の水準を損なわないことが求められる。

拡張イーサネットは，FC フレームをカプセル化しているが，フロー制御は拡張イーサネットの方式を使用することが規定されている。従来の FC-2 層のクレジット方式のパラメタは使用せず，無視している。

既存のイーサネットは，隣接ノード間でフロー制御（IEEE 802.3x）を行っている。これは，クレジット方式のような，相手のバッファの容量を考慮に入れた方式ではない。自分のバッファが枯渇しそうになったら，PAUSE フレームを送り，物理リンクのトラフィックを一時的に止めるように相手に通知する仕組みしかもたない。

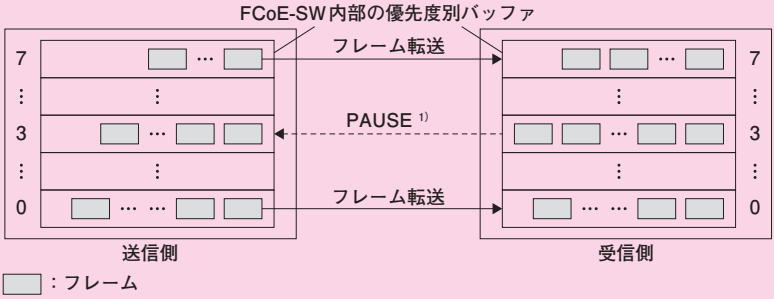
これでは，統合ネットワークにおいて，ストレージトラフィックの信頼性を確保するには不十分である。なぜなら，統合ネットワークでは，ストレージトラフィックや IP トラフィックなど，優先順位の異なるトラフィックが同じ物理リンク上を流れるからである。

TCP はウィンドウ制御を行っているが，これをエンドシステム間で行っているので，局所的なバッファ枯渇には対応し切れない。そのため，経路上のどこかで輻輳しているにもかかわらず，パケットを送り続ける可能性を秘めている。輻輳している場所がイーサネット上であれば，隣接ノード間で IEEE802.3x のフロー制御が働く。この結果，リンクを流れるトラフィックの種類を識別することなく，物理リンク全体のトラフィックを止めてしまう。イーサネット上で輻輳したら，ストレージトラフィックも影響を受けてしまうのだ。

そこで，拡張イーサネットは，IEEE802.3x の仕様を拡張し，FC-2 層のクレジット方式に代わる新しいフロー制御の方式を規定した。それは，「仮想リンクごとの優先度付きバッファ制御」（PFC），「仮想リンクごとの帯域制御」（ETS），「スイッチ間のプロパティ交換」（DCBX）の三つである。

- **仮想リンクごとの優先度付きバッファ制御**
  まず，1 本の物理リンク上に最大 8 本の仮想リンクを構築し，仮想リンクごとに，優先度付きのバッファをもたせる

機能を追加した。ノードは，自分のバッファが枯渇しそうになったら，優先度の低い仮想リンクの通信を一時的に止めるようにPAUSEフレームを送る仕組みを備えている。



注1)　受信側バッファの枯渇を防止するために送出する。
注記　0～7の数字は，バッファの優先度を示す。数字が大きいほど優先度が高い。

図：優先度付きバッファ制御機能(平成23年午後Ⅱ問1の図5より作成)

試験に出る

優先度付きバッファ制御の仕組みについて，平成23年午後Ⅱ問1で出題された。ただし，本文の中でこの仕組みは詳しく解説されており，従来技術のPAUSEフレームの知識から推論できるように配慮されていた

ある優先度のバッファが枯渇した場合，どうなるだろうか。当該優先度の通信だけを抑止できるので，他の優先度の通信に影響を及ぼさないようにできる。

この結果，優先度の高い通信と低い通信が同時に発生した場合，低い方の通信が大量であったとしても，低い方の帯域を一定量以下に抑えることができる。なぜなら，あらかじめ設定しておいたバッファ容量が枯渇した時点で，PAUSEフレームが送出され，低い方の送信が抑止されるからだ。その結果，優先度の高い方の通信が妨害されることはない。

トラフィックに優先順位を付与する機能は，PFC（Priority-based Flow Control，優先度ベースのフロー制御）と呼ばれ，IEEE802.1Qbbで規格化されている。

物理リンクを流れるパケットがどの仮想リンクを流れているか(つまり，どの優先順位が付与されているのか)をスイッチが識別するため，パケットのVLANタグ（IEEE802.1Q）にある優先度フィールドを使用する。

詳説

PFCの優先度は，拡張イーサネットフレームにはVLANタグの優先度フィールドに設定される。拡張イーサネットフレームの送信端末が特定のVLANに属さない場合，VLAN IDを「0」に設定する。
VLANタグについて，詳しくは第1章「1.4.2 VLAN」を参照していただきたい

- **仮想リンクごとの帯域制御**
  拡張イーサネットは，優先度付きバッファ制御に加え，仮想リンクごとに帯域制御を行う機能も追加している。
  トラフィックごとに帯域制御を行う機能は，ETS（Enhanced Transmission Selection，拡張伝送選択）と呼ばれ，IEEE802.1Qaz で規格化されている。
  PFC と ETS により，統合ネットワークにおいて，ストレージトラフィックの「ロスレス」を実現できる。ストレージトラフィックを流す仮想リンクに対し，高い優先順位と一定の帯域を与えればよいからだ。
- **スイッチ間のプロパティ交換**
  各スイッチが PFC と ETS を装備していようとも，隣接するスイッチ間で，PFC と ETS の設定情報の整合性がとられていないならば，FC-SAN のクレジット方式に比肩する Buffer-to-Buffer のフロー制御を実現できない。
  拡張イーサネットは，IEEE802.1AB（LLDP：Link Layer Discovery Protocol）の機能を利用して，拡張イーサネット対応スイッチ間でプロパティの交換を行うことができる。これは，DCBX（Data Center Bridging Exchange）と呼ばれている。

2.4.3 リモートバックアップ

広域災害時の事業継続性を確保するため，信頼性の指標として，**目標復旧時点**（**RPO**：Recovery Point Objective）を定めることがある。

RPO とは，障害発生時点から遡って，どの時点までデータを復旧するかを定めた目標値である。例えば，RPO を 24 時間に定めた場合，障害発生時点から 24 時間以内の業務データが復旧の対象となる。

試験に出る
RPO について，平成 26 年午前Ⅰ問 21 で出題された

●RPO を 24 時間に定めた場合の対策

広域災害を想定して RPO を 24 時間に定めた場合，その具体的な対策として，被災を免れる遠隔地に副系拠点を設け，主系拠

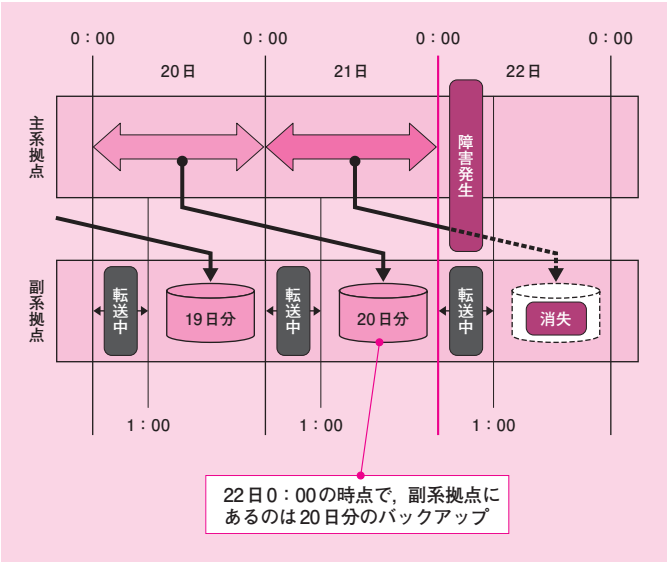
点の 24 時間以内の業務データを副系拠点にバックアップしておく方法が考えられる。

このとき，ネットワーク回線を経由して業務データを副系拠点に転送するのであれば，転送の所要時間を考慮に入れて，バックアップ取得の間隔と頻度を計画する必要がある。

例えば，24 時間無停止で業務を行っている例を取り上げてみよう。主系拠点の 1 日分の業務データ（前日 0：00 ～本日 0：00 の直前）を毎日 0：00 から転送するものとし，その所要時間が 1 時間であるとする。

22 日の 0：00 の時点で，20 日分の業務データが副系拠点にバックアップされている。

22 日の 0：00 から，21 日分のバックアップを開始する。その転送を行っている最中（0：00 ～ 1：00）に主系拠点が被災するならば，どうなるだろうか。



図：バックアップ転送のスケジュール

障害発生以前の全データが主系拠点で消失する可能性，及び，今まさに転送中の前日分データがネットワーク回線で消失する可能性がある。被災を免れているのは，副系拠点で安全に保管された一昨日までのデータなので，この方法では 24 時間という

RPO を満たすことができない。

したがって，この例においては，バックアップデータの転送を1日2回以上実施する必要がある。

●RPO を 0 時間に定めた場合の対策

RPO を 0 時間に定めた場合は，データの消失を一切許容しないことを意味する。

その具体的な対策として，主系拠点から副系拠点に向けて，**同期式コピー**を取る方法が考えられる。

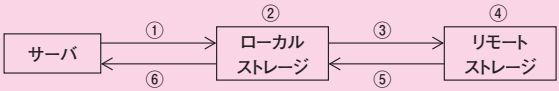
同期式コピーでは，主系拠点のサーバからローカルストレージに書込み命令を出すと，副系拠点のリモートストレージにも書込み命令が出される。そして，リモートストレージからの書込み完了通知を待って，ローカルストレージはサーバに書込み完了通知を行う。つまり，ローカルストレージとリモートストレージは同期を取っている。

平成 20 年午後 I 問 2 には，リモートコピーの方式として，同期式と非同期式を比較する問題が出題されている。参考までに該当箇所を掲載する。

試験に出る

重複排除の技術を用いたリモートコピーについて，平成 22 年午後Ⅱ問 1 で出題された

リモートコピーの方式には，同期式と非同期式がある。同期式コピーは，リモート側でのデータ更新を待ってサーバに更新完了報告を行う方式であり，非同期式コピーは，リモート側でのデータ更新完了に左右されずに更新完了報告を行う方式である。図1に，同期式コピーの仕組みの例を示す。



処理順序
①ローカルストレージへの書込み命令
②ローカルストレージでの書込み処理（T_1）
③リモートストレージへの書込み命令（T_2）
④リモートストレージでの書込み処理（T_1）
⑤リモートストレージからの書込み完了通知（T_3）
⑥［　a　］

T_n：処理時間
注　②と③は同時に実行される。

図1　同期式コピーの仕組みの例

図1では，⑥の実行によってデータ更新が完了するので，障害発生直前のデータまで保証される。しかし，ネットワークでの遅延や送受信におけるエラーリカバリ処理などによって，サーバの［　オ　］が低下する。ネットワークでの遅延は，機器や伝送媒体の性能にも左右されるが，光の速度（約 3×10^5km／秒）そのものが制約となり，距離に応じて発生するので，バックアップサイトとの距離を考慮する必要がある。

図：リモートコピーの方式（平成20年午後Ⅰ問2より引用）

ここには，「⑥の実行によってデータ更新が完了するので，障害発生直前のデータまで保証される」と記述されている。したがって，この方式を採用すると，RPOを0時間にすることができる。