3.10 共有ディスクのメッシュ接続に関する教訓（T10）

教訓 T10　メッシュ構成の範囲は、可用性の確保と、障害の波及リスクのバランスを勘案して決定する

問題

A 社の、サーバと NAS をフルメッシュ接続したシステムにおいて、局所的なディスク障害がシステム全体に波及し、すべてのサーバがダウンした。サービス再開までの間、トランザクション処理が中断した。

システムの概要は次の通り（図 3.10－1）。

- あるサービス用のシステムにおいて、性能及び可用性確保のため複数のサーバと 8 基の NAS をフルメッシュで接続していた。

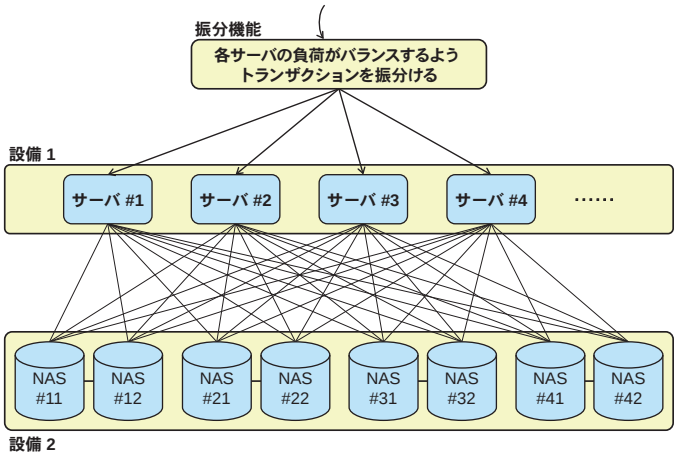


図 3.10－1　フルメッシュ構成のイメージ

- NAS #11 と #12、～ #41 と #42 はそれぞれペア（4 ペア）を組み、同時並列稼働（アクティブ / アクティブ）している。各ペアには、処理対象クラスのインスタンスが分散して保管されている。
- ペアの一方に障害が発生した際には他方で処理を引継ぐ（図 3.10－2）。

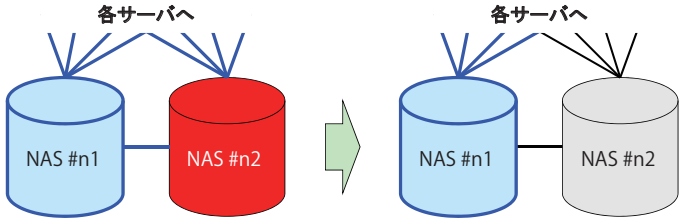
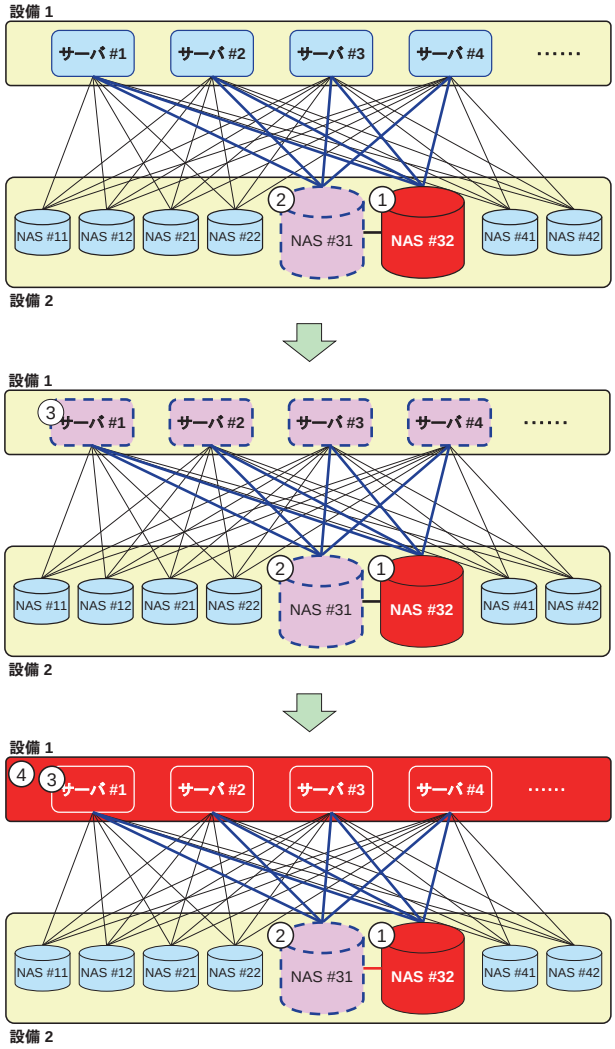


図 3.10－2　ペア構成。障害時にはペアの一方が処理を引継ぐ

障害発生の経緯を図 3.10－3 に示す。



NAS#31, #32 のペアにおいて、

① NAS #32 にハードウェア障害が発生。

② ファームウェアの不具合（バグ）により、#32 を切り離すことができず、NAS #31 への処理引継ぎ、切替えが完了できない状態となった。

③ フルメッシュ構成であったため、すべてのサーバにおいて NAS #31 のマウントポイントが「外れている」と認識された。

④ そのまま時間が経過し、全サーバがダウンした。

図 3.10－3　障害発生の経緯

原因

直接的な原因はフルメッシュ構成そのものにある。すべての NAS がすべてのサーバに接続されていたため、NAS コントローラファームウェアの不具合により障害ディスクの切離しに失敗したことがシステム全体に影響を及ぼし、全サーバのダウンにつながった。

根本的な原因は、フルメッシュ構成のリスクについて充分に考慮しないまま採用したことにある。メッシュ構成により理論上の信頼性（可用性）は向上するが、ネットワークを構成する機器・装置の一

部に発生した障害が、メッシュ化された全領域に波及する危険性も増大させる。サービス提供者として、許容可能なリスクの程度についての事前検討が必ずしも十分でなかった。

対策

本事例において、実際に行われた対策は次の通り。

- 暫定処置として、トラフィックを BCP 設備へ迂回させることによりサービスを継続した。
- NAS コントローラに対してファームウェアの機能修正パッチを適用した。
- 類似障害の再発防止のため、局所的な障害により全サーバがダウンするような事態を回避するため、フルメッシュ構成を見直した。
  - 1 基のサーバと 2 ペアの NAS を接続した「グループ」から成る構成に改めた。
    一部のデータにアクセスできなくなっても、他のデータに対するトランザクション処理は継続できるようにした（図 3.10－4）。

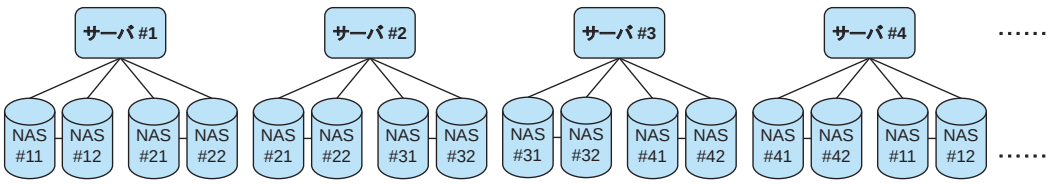


図 3.10－4　サーバと NAS のグルーピング例

  - グルーピングに対応して、振分機能を、単なる負荷分散から、各サーバが接続する NAS に応じてトランザクションを振分けるように改修した。

グルーピング後のシステム構成のイメージを図 3.10－5 に示す。

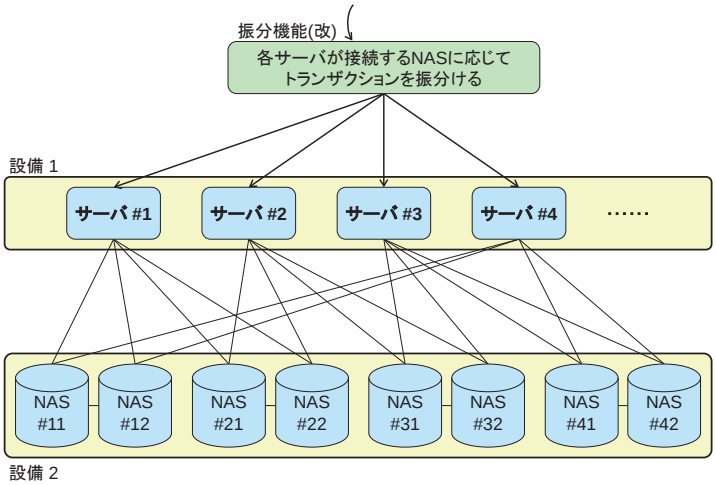


図 3.10－5　メッシュ化見直し後のシステム構成

- さらに、再発防止策ではないが可用性を担保するための施策として、迂回時の性能劣化を防ぐため、BCP 設備を増強した。

効果

NAS の局所的な障害が波及する範囲が限定されたことにより、同様の障害によりすべてのサーバがダウンするリスクは低減された。

教訓

- メッシュ構成により可用性の向上が期待できる。一方で局所的な障害が全体に波及するリスクも増大する。安易にフルメッシュ化するのではなく、目的に応じた最適な構成を検討することが望ましい。
- 本稿に揚げた構成は対策の一例であり、グルーピングの単位、メッシュ化対象範囲の考え方等については個別に検討されたい。