3.22 バッファプールの管理に関する教訓（T22）

教訓 T22　隠れたバッファの存在を把握し、目的別のしきい値設定と超過アラート監視でオーバフローを未然に防止すること

問題

A 社は 24 時間 365 日予約受付システムを運用している。複数種類の業務の予約を同時に受け付けており 1 日の受付数は平均約 10,000 件／日、ピーク日は 30,000 件／日である。

ある日の夜間、業務予約処理 A のバッファが処理待ちで滞留し、予約受付システムからの転送が停止していた。暫くすると、通常処理できていた予約処理 B と C も受付ができなくなり、すべての予約処理の受付が停止する状況となった。A 社の予約受付システムの構成概要と問題の発生状況は図 3.22－1 のようになっている。

処理概要を以下に示す。

- 稼働系と交代系のホットスタンバイ構成で交代系に切り替えてもバッファの内容は引き継がれる
- インターネットからの受付処理により、チェック・登録された入力データは共通バッファに入れられる
- 共通バッファから振分処理で随時入力データを仕分けし、予約処理ごとの転送バッファに格納する
- 各転送処理は転送バッファに登録された入力データを予約処理サーバに転送する
- 予約処理サーバは転送された入力データで予約データベース（以下、予約 DB）を更新し、インターネットを通して回答を端末に返却する。

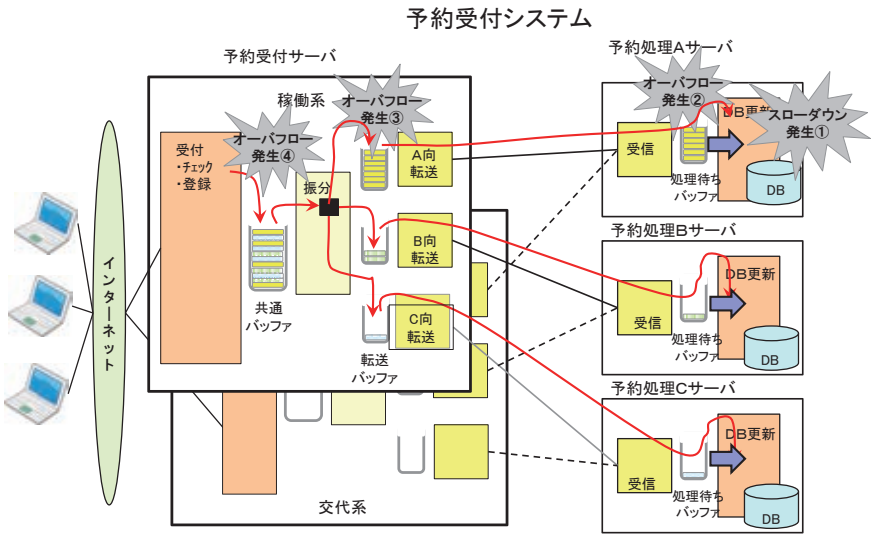

図 3.22－1　システム概要と障害の発生状況

原因

予約処理 A の受付はこの日から開始されたものであった。予約処理 A サーバの処理がメモリ不足により、スローダウン状態となった（図 3.22－1①）ため、処理待ちバッファに徐々に入力データが滞留し、上限の 1,000 件を越えた（図 3.22－1②）。これにより、予約受付サーバ側の転送バッファに未送信データが滞留して満杯となり（図 3.22－1③）、共通バッファから予約処理 A の入力データが取り出されなくなり、共通バッファも満杯となり（図 3.22－1④）全予約処理の受付が停止した。スローダウンが発生してから、受付が停止するまで 30 分程度の時間差があった。

この障害発生過程において、予約受付システムの共通バッファが満杯になった段階で、すべての予約受付業務を停止するメッセージが表示されたため障害が発生していることが判明した。

予約受付システムは、予約処理の種類ごとに受付中／受付停止を設定することは可能であったが、問題が起こった予約処理 A のみを受付停止する前に全予約業務停止となってしまった。さらに、交代系に切り替えてもバッファの内容は引き継がれるため、このケースでは復旧できなかった。

対策

① 復旧措置

予約業務 A サーバのスローダウン状態を設定変更により回復させ、滞留している入力データを順次処理していくことにより、2 時間程度かけて共通バッファを空にした。この後、予約受付システムを再開し、通常運用に戻った。

② バッファオーバフロー状態の検知

障害状況を早期に検知できなかったシステムの問題に対しては、各バッファの蓄積状況を監視し、警戒レベルに達したら監視コンソールにアラートを表示するようシステムの改善を実施した。

効果

バッファへの入力データの滞留状況を監視し、異常な状態を早期に検知することでシステム障害の発生を未然に防止することが可能になった。

一般的に情報システムはメッセージをプロセス間でバッファを用いて受け渡すバケツリレー方式となっていることが多い。（図 3.22－2）

よって受け取り側のプロセス処理が遅れたり、停止したりするとバッファにメッセージが滞留していくことになる。システムが良好なパフォーマンスを維持しているかどうかはこのバッファの滞留状況を監視し適切な状態であることを評価することで判断できる。

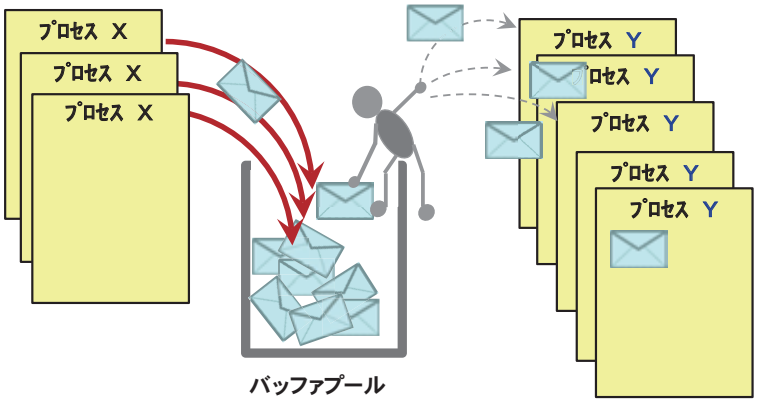

図 3.22－2　バッファを経由したプロセス間通信

このバッファがオーバフローすると、プロセスＸからのメッセージ登録ができなくなりシステム障害となることが多い。よって、バッファの蓄積状況を監視し、一定のしきい値を超えたら監視コンソールにアラート情報を表示することが有効であり、しきい値は注意レベル、警告レベル、危険レベルのようにレベルを分けアラート情報の緊急度も合わせて表示することが望ましい。

なお、しきい値の設定にあたっては、プロセスＸとプロセスＹの連携度合いにより適切な値を検討する。

リアルタイムに近いメッセージ連携形態の場合は数件蓄積されただけでも異常が発生している可能性があるが、メッセージの登録が時間帯によってピーク性がある場合には 70% ～ 80% 程度まで許容範囲とみなすことができるので、それぞれの適切なタイミングでアラートを表示するよう設計を行う。

また、各バッファのサイズ（最大収納件数）は構成情報として管理し、稼働状況や業務要件の変化等に応じて見直しを行う。

通常の１日単位で運用されるシステムでは、システム開始時にバッファは空であり、稼働中のバッファは増減を繰り返すが、システム終了時に空に戻る、あるいは終了時点で蓄積データが存在した場合には後処理で対応を行う。しかし、24 時間連続稼働のシステムではこのバッファは常に増減をしているため、管理には特に注意し、オーバフローを未然に防止しなければならない。

また、パッケージ製品を利用する場合はバッファが明示されないことがあるため、どこに何のバッファが存在しているかを把握することも必要である。

教訓

本システムのような共通バッファのオーバフローに起因するシステム障害から得られる教訓は以下のとおりである。

○各種バッファの存在を認識し、構成情報としてその最大収納件数を認識・管理する。
　特にパッケージ製品を利用する場合は明示されていない内部バッファの存在を把握しておく必要がある。

○用途別にしきい値を設定し、しきい値を超えた場合にアラートを表示することでオーバフローによるシステム障害を未然に防止する。