## 3.18 既存システムとのデータ連携に関する教訓（T18）

### 教訓 T18　新たなサブシステムと老朽化した既存システムとを連携する場合は両者の仕様整合性を十分確認すべし



#### 問題

A社のシステムは日中のオンラインと夜間バッチで構成されている。日中のオンラインにより受け付けたサービス要求を夜間バッチに連携し、そのサービス実行処理を完結する流れとなっている。

ある日、特別な事象が契機となり、オンラインで大量の入力処理が集中した（図3.18－1①）。

しかし、オンラインではデータ制限がなされておらず、そのまま夜間バッチに連携されたが、夜間バッチの処理能力の制限値を超えたため異常終了した（図3.18－1②）。

その制限値を拡大して夜間バッチを再実行したが、異常終了時に欠落したデータの復元作業が難航し、夜間バッチ処理に予定以上の時間を要した（図3.18－1③）。

ぎりぎりの時点での判断により、翌朝の通常時刻でオンライン処理を開始するため、夜間バッチを中断しバッチからオンラインへの切替えの実行に着手した（図3.18－1④）。

強制中断の結果、以降の（あるいは，残存した）バッチの自動運行ができなくなり、手動で夜間バッチを実行せざるを得なくなった（図3.18－1⑤）。

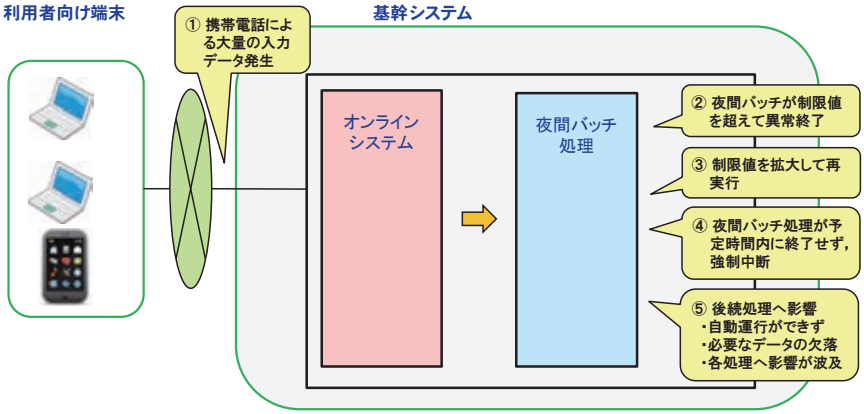


図3.18－1　障害の経緯

この結果、膨大な作業が発生し、処理失念や誤処理による多数の副次的障害も発生した。これにより、翌日のオンライン開始処理とこれにともなう各種の処理が大幅に遅延した。この状況は1日では回復せず、影響は日を重ねるごとに広がり、収束までに10日間を要した。顧客への影響としては、オンライン業務のサービス開始が遅延、及びサービス停止となり、一部のサービス明細が欠落することとなった。

## 原因

直接の原因は、夜間バッチの処理能力の制限値を超えたため異常終了したことである。

携帯電話からのバースト的なサービス要求（あるいは，サービス利用）データが無制限に受け付けられて、後続のバッチシステムに連携された。

根本原因は以下である。

バッチシステムの１日の処理量には上限が存在すること、それを超過した場合は異常とみなし処理停止することが確認できていなかった。また、バッチ処理を一旦強制中断させると以降の処理の自動運行はできず、手動によらざるを得ないことも把握できていなかった。

## 対策

本件に対する再発防止策を以下に示す。

(1) 既存システムの要件定義の有無と要件定義の内容を再度チェックして見える化し、これをもとに現在の環境との整合性や、新たなサブシステムを構築して既存システムと連携する場合は両者の整合性を確認する。これらの事項を盛り込んだルールを作成しマニュアルに取りまとめる。

さらに、以下についても実施しておく。

(2) システムが異常終了しても途中から再開始可能な仕組みと対応手順をあらかじめ考慮しておき、異常終了してもシステムが誤動作せずに制御できるようにする。

## 効果

全体の視点で既存システムの要件を見える化したため、新システムの追加による既存システムへの影響が明確化され、障害の連鎖回避、影響の極小化などが実現できた。

## 教訓

老朽化した既存システムは、仕様・制限等が不明確になっていることがある。既存のバッチ処理システムに対しフロントにオンラインシステムを追加する場合や、フロントのオンラインシステムを機能拡張する場合は、制限値を超えたときのチェック方法や、既存のバッチ処理システムが異常終了しないかどうかについて、両者の整合性を十分確認する必要がある。