

3.15 データの一貫性確保に関する教訓 (T15)

教訓
T15

緊急時こそ、データの一貫性を確保するよう注意すべし

問題

A社が提供するWebサービスにおいて、顧客ごとのサービス利用状況と人口統計データを組み合わせて分析し、顧客を分類するためのカテゴリ判定に不正が生じた。修正対応までの約1日間、一部の顧客に対して不適切なカテゴリが適用された。

カテゴリ判定処理の概要は次の通り(図3.15-1)。

- カテゴリ判定・適用は毎月末に夜間バッチ処理で行う。
- ①事前に顧客データ(オンライン)から作成した顧客データ(バッチ処理用)、②顧客別の月次取引実績、③外部から取得する人口統計データを用いて、各顧客のカテゴリを算出する。
- 結果を顧客データ(オンライン)に反映する。

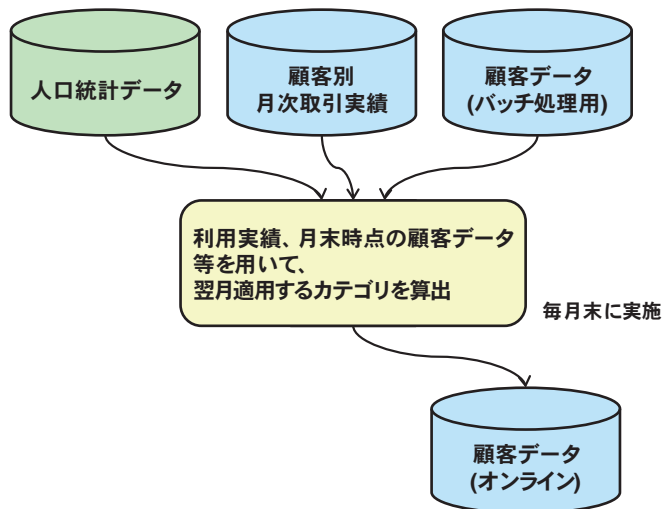
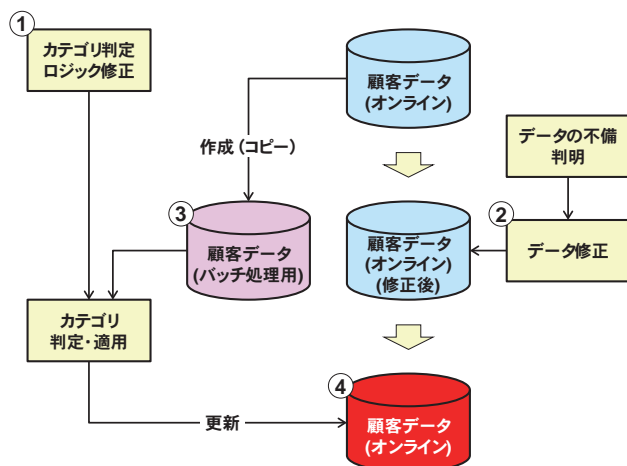


図 3.15-1 処理の概要

障害発生の経緯を図3.15-2に示す。



- ① カテゴリ判定ロジックを修正した。
- ② 新ロジックに対応するためのデータ移行の際に顧客データの不備が判明。業務部門の依頼により、緊急作業として顧客データ（オンライン）に対し修正を行った。
- ③ このとき、既に作成済みであったカテゴリ判定バッチ処理用顧客データは修正または再作成されなかった。
- ④ 月末にそのままカテゴリ判定処理を行い、顧客データ（オンライン）を更新したため、一部の顧客について誤ったカテゴリが適用された。

図 3.15 - 2 障害発生の経緯

原因

直接的な原因は次の通り。

- カテゴリ判定に用いる顧客データ（バッチ処理用）の内容に不備があった。当該データの源である顧客データ（オンライン）に対する修正が顧客データ（バッチ処理用）に反映されていなかった。

根本的な原因は次の通り。

- 顧客データ（オンライン）の修正が異例かつ緊急を要するものであったため、影響範囲の事前調査が不十分であった。
- 修正作業及び関係各所への報告に意識が集中し、後続する通常業務への引継ぎが疎かになった。
- データ更新時の影響確認を効率化するための、原本（マスタ）と複製（コピー）の対応表等の情報が整備されていなかった。

対策

本事例において実際に行われた対策は次の通り。

- 直接的な対策
 - － 修正済み顧客データに基づくバッチ処理用データを作成。カテゴリ判定を再実行した。
- 類似障害の再発防止策
 - － 緊急時対応に際して、通常業務とは異なる手順、内容の作業を行うことの影響範囲を見極め、対応結果が後続する平常時の業務及びシステム運用の流れに確実に繰り返されるよう、確認手順、テストケースの洗出し等を特に意識的に行う旨周知した。

効果

- 直接的な対策により、一部顧客に対する不正なカテゴリの適用は約1日で解消された。
- 再発防止策により、緊急時対応の影響により後続の通常業務に支障を来すような事態は少なくなると期待できる。

教訓

システム内には、ある原本（マスタ）データに対して、業務プロセスやアプリケーションの必要に応じて、複数の複製（コピー）データが存在する。これらの原本及び複製は、各業務における追加・更新・削除等を通じて、一貫性（インテグリティ）が保たれなければならない。

一貫性を確保するためには、原本とそこから派生するすべての複製の対応関係を把握し、各業務プロセスを通じてそれぞれのデータがどのように同期、更新される必要があるかについて整理し、作業時に参照する、あるいは必要に応じてツール等を利用して自動的にデータが同期、更新されるよう、作業ルール・手順等を明確化し、環境を整備する必要がある。

通常業務について、上記のような作業手順・環境を整備済みの組織であればなおさら、緊急時対応の影響により一貫性が破綻するような事態は避けたい。自動化の要否については管理対象の重要性やコストを勘案して個別に決定すれば良いが、少なくとも緊急時対応において、以下の点に十分な注意を払い、作業手順等に定めておくことが望ましい。

- 作業開始時に、一貫性の観点から影響を受けるデータを把握しておくこと
- 作業終了時に、それらのデータを同期させ、後続の通常業務に支障を来さないようにすること