

3.20 パッケージ製品の機能カスタマイズに関する教訓 (T20)

教訓
T20

パッケージ製品の機能カスタマイズはリスクを認識し特に必要十分なチェック体制やチェック手順を整備して進めること

問題

A社は24時間365日コールセンター受付システムを運用している。コールは会員からの作業員派遣要請が主でその内容により最寄りのサービス拠点から作業員が現場に駆け付けて対処するものであり、1日のコール数は平均約3,000件であり連休の際には特に集中する。

連休中のある日の12時頃、オペレータが受付端末のタッチパネルが反応しなくなっていることに気づいた。また利用者からコールが繋がらないとのクレームも数件寄せられていた。本事象は同じ構成を持つ交代系システムへの手動切替えを実施し回復するまで約10分間継続していた。この間のコール数は不明だが、直前の10分間では20件のコールが発生していた。

このコールセンター受付システムは新システムに更改してから1週間連続稼働していた。新システムは手作りで構築された旧システムと異なり、ベンダのパッケージ製品ソフトを導入し構築されたが、A社の要求仕様に対応するためベンダは機能追加^{*1}のカスタマイズを実施していた。

システムの構成の概要は以下のとおり(図3.20-1)。

- 電話系の呼処理を制御するデジタルPBXサーバ
- 電話コールに連動して受付端末の画面を制御するCTIサーバ
- 各サーバは現用系と交代系の二重化構成

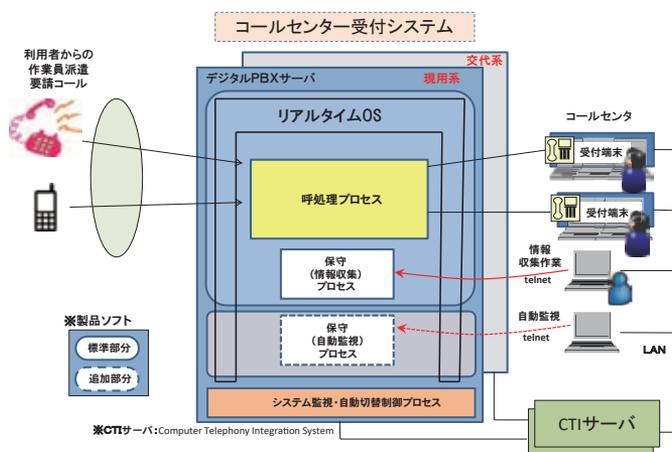


図 3.20-1 コールセンター受付システムのプロセス構成概要

^{*1}telnetによる呼処理プロセスの稼働状況を自動監視する機能、デジタルPBXサーバ内に実装(図中の「保守(自動監視)プロセス」)

原因

デジタル PBX サーバを交代系に手動切り替えし回復させた後で、ハンガアップ状態であった現用系のシステムダンプを取得し解析した結果、保守員が行った障害情報収集のための telnet 接続と呼処理の稼働状態を自動監視するための telnet 接続が競合し無限ループ状態に陥ったことが原因であると判明した。また、システムの異常を検知して交代系システムに自動的に切り替える機能もソフトウェアの不具合から無限ループを検知できなかつたため作動しなかつた。障害の発生状況を図 3.20-2 に示す。

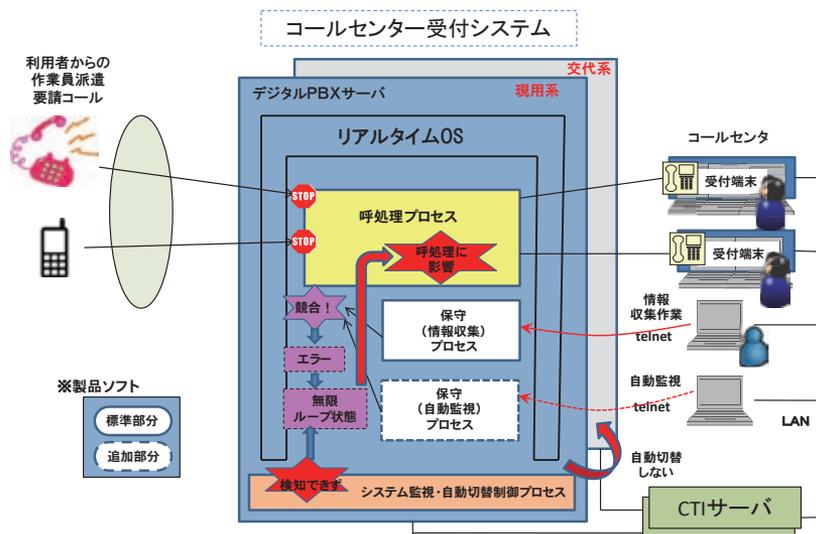


図 3.20-2 コールセンター受付システムの障害状況

調査の結果、telnet の競合は希少なタイミングで発生するコールセンター受付システムのファームウェアのプログラム不具合と判明した。また、交代系への自動切替えが出来なかつた事象は自動切替え制御機能の不具合が原因であるとベンダから報告された。

なお、本システムの構築にあたりユーザである A 社から提示された要求仕様を満たすために、ベンダは同業他社でも広く利用されているパッケージ製品ソフトをベースにカスタマイズを実施したが A 社に十分な説明がされていなかつた。

対策

本システム障害事例でとられた対策を以下に記す。

① 直接原因と復旧措置

コールセンター受付システムのファームウェアの不具合によるシステムハンガアップがサービス停止の直接原因であった。交代系への手動切替え実施により復旧し、受付サービスを再開した。

② プログラム不具合への対応

問題を起こしたファームウェアのプログラム修正を行い、再現テストを繰り返して検証し 4 日後に本番環境に適用した。

③ 2つの telnet 接続の競合への対策

機能追加した呼処理自動監視プロセスへの接続は telnet プロトコル方式をやめて、RS232C 回線による接続方式に変更し競合が発生しないように対処した。

④ FTA 分析¹¹を活用した総点検

同様の競合発生個所の有無について、FTA 分析手法を活用した総点検を実施し、同様の不具合を数件検出、対策計画を策定し、緊急性に応じて順次対策を実施している。

効果

前述の対策により、障害は再発せず順調に稼働している。また、telnet 接続を本来のパッケージ製品ソフトの仕様どおり 1 本にしたことから、同種の製品を使用している同業他社と同様の信頼性を確保したと考えられる。

教訓

今回の障害はシステムを刷新し、稼働を開始した直後の初期トラブルであるが、非常にまれなタイミングで発生する競合が引き金になったものであり、事前のテストでは検出が困難であった。同業他社でも使用されている信頼性の高いパッケージ製品ソフトを採用していたが、呼処理の自動監視をする要求仕様に対応するため、このパッケージ製品ソフトに機能追加を実施しており、そのプログラム不具合が競合発生の原因となった。ベンダは発注者に対してこの機能追加にともなうリスクを共有し、改造個所の処理方式を説明し、必要十分なチェック体制とチェック手順を整備して進めることが重要である。

¹¹ FTA 分析 (Fault Tree Analysis: 故障の木解析)