2.16 本番環境における作業ルールに関する教訓（G16）

教訓 G16 本番環境へのリリースは、保守担当が無断でできないような仕組みを作るべし！

問題

世界中に顧客を持つグローバル企業 A 社は、いつでもどこからでもサービス要求を受付可能な 24 時間運転の Web システムを運用している。ある日、システム障害が発生したことにより、数十分間、サービス要求を受け付けられない状態となった。

本システムの構成（概要）を、図 2.16－1 に示す。

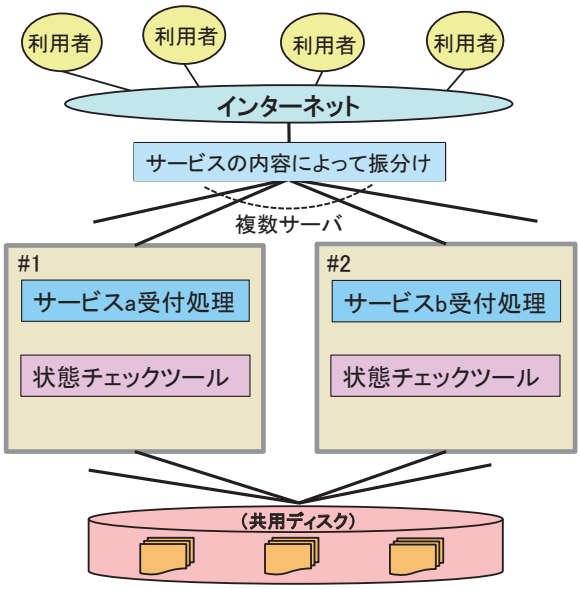

図 2.16－1　本システムの構成（概要）

① システムの構成について

サービスの種類ごとに、「サービス a 受付処理」、「サービス b 受付処理」等、それぞれサーバが別々に処理を行っている構成である（図中には 2 号機までしか示されていないが、実際はさらに複数のサーバで構成されている）。共用ディスクは、ユーザが送信したデータを一時的に保存しておく領域で、夜間バッチで顧客 DB に登録される運用となっている。（システム構成図に顧客 DB は書かれていない）

② 状態チェックツールについて

図 2.16－1 に桃色で示した状態チェックツールは、サーバの稼働状態（リソース使用状況、ディスク転送速度等）をチェックするツールである。本ツールは、使用頻度がそれほど高くないことから、現状、各サーバ上で手動にて起動する運用となっている。

③ 運用・保守の体制について

本システムは、ベンダに保守と運用を一括委託しており、24 時間体制で運用を実施している。アプリケーション資産の変更、システムへの機能追加など、システムの変更をともなう作業については、A 社主体のシステム変更会議による審議・承認を得る規則となっている。しかし現状、審議対象案件の明確な規定はなく、どの程度の変更ならば会議に諮るかは属人的な判断となっている。

原因

システム障害が発生した経緯について、図 2.16－2 に示す。

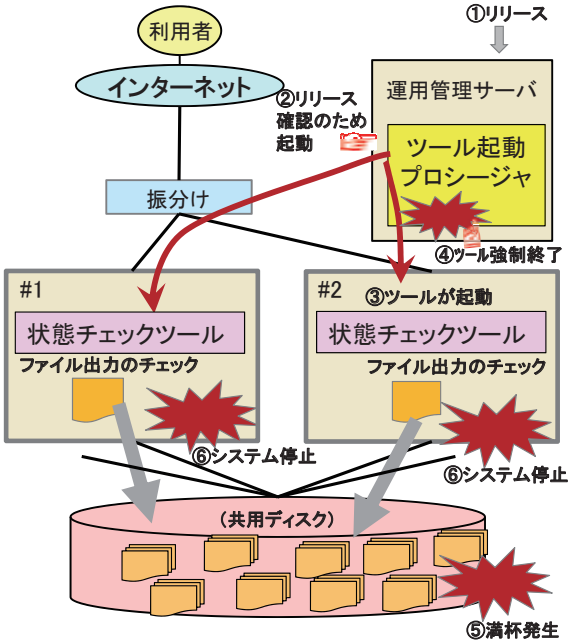

図 2.16－2　システム障害が発生した経緯

① 作業の負荷軽減を目的として、各サーバ上で手動にて起動している状態チェックツールを、一括で起動可能とするツール起動プロシージャ（バッチファイル）を作成し、運用管理サーバにリリースした。
② プロシージャのリリース確認のため、システムのオンライン中にこのプロシージャを起動した。
③ 各サーバで状態チェックツールが起動されたことを確認した。
④ 確認は済んだと認識し、各ツールの完了を待たずにプロシージャを強制終了した。

⑤ ツールが行うチェック項目の一つとして、共有ディスクへの書き込み出力機能のチェックがあるが、ツールが正常に終了しなかったことにより、この機能が繰り返し起動される状況となってしまった。程なくして、共有ディスクはツールの同機能が出力するテストファイルにより一杯となった。
⑥ 当該ディスクを共有するすべてのサーバがシステム停止に至った。

なお、作業担当者は、今回の作業はシステム変更会議への付議が不要な運用改善作業の位置付けと考え、会議に付議していなかったため、A 社側では当該作業が行われていることを認識していなかった。

本事象に対して、ベンダから以下 3 点の原因及び対策が示された。

【原因 1】当該作業は本来、システム変更会議に諮るべき内容の案件だったにもかかわらず、判断を誤ってしまった。具体的には、作成したものは運用改善のための簡単なバッチファイルであり、確認作業も問題なくすぐに終わるはずなので、会議に諮るほどのことはないと安易に考えてしまった。
【対策 1】システム変更会議に諮るべき作業対象を明確化する。

【原因 2】当該プロシージャを作成した担当者と、リリース作業を実施した担当者が異なっており、プロシージャを強制終了することによってどのような影響が出るかについて、情報の共有ができていなかった。
【対策 2】リリース作業担当者は、自分が扱うものについて、その動作条件を十分に確認した上で実施することを徹底した。

【原因 3】「ツールの強制終了」という、作業手順書に書かれていないことを実施してしまった。
【対策 3】作業手順書に書かれていない操作を禁止する。また、作業ルールに関する継続的教育を行う。

A 社はベンダからの報告を聞き、再発防止への対策はこれで本当に十分かを検討した。検討の結果、A 社は、保守作業担当者が承認なしに本番環境で作業を行っていたことがそもそもの問題ではないかと考えた。たとえ会議に諮る作業の対象を見直したとしても、個人の判断に委ねられる部分が残る限り、再発のリスクが残るからである。

対策

A 社は、再発防止策を以下のとおりとし、実施のためのルールを策定した。

○再発防止策

本番環境へのリリースは、保守担当が無断でできないような仕組みを作る。

○策定したルール

- 保守担当は、作業実施にあたってログイン ID の払い出しを受けなければならない。（作業ごとにログイン ID は異なる）
- ログイン ID の払い出しを受けるために、保守担当は作業内容について、A 社主体のシステム変更会議に必ず諮らなければならない。
- システム変更会議には、以下の内容を含む保守作業計画書の提出を必須とする。記載内容について、関係者と情報を共有し、当該変更部分の有識者を交えたレビューを行う。

  ※保守作業計画書に記載すべきもの：作業の目的、テスト環境における作業実施結果、作業タイムチャート、作業実施体制、作業手順（作業結果の確認方法を含む）、万が一の際の戻しの判断基準、連絡体制、ログイン ID 払い出し申請
- システム変更会議で承認を受けた作業手順以外のことを実施してはならない。（作業手順書に書かれていないことを実施してはならない）

効果

この対策を実施してから、A 社が認識していない作業によるシステム障害は発生していない。

教訓

本番環境へのリリースは、保守担当が無断でできないような仕組みを作るべし！

なお、今回の問題を引き起こした保守担当者は、作業効率の向上という現場改善意識から自ら工夫を行った。その手順に不適切な点があったが、作業改善の意欲自体は悪いことではない。もしかしたら、この担当者は、これまでに数々の改善を実践してきたかもしれない。この問題だけを契機に管理を厳しくするあまり、現場の改善意欲を委縮させることは好ましくない。再発防止施策のバランスについての配慮も重要であることを付記しておく。