2.8 共同利用システムの利用者間情報共有に関する教訓（G8）

教訓 G8　共同利用システムでは、非常時対応を含めて利用者間の情報共有を図ること

問題

教訓 G7 と同じ事例である。本教訓で特筆すべきこととしては以下があげられる。

A 社と D 社は、あらかじめ協議を行い、運用コスト削減という目的が一致したことからシステムを共同利用することとした。

B 社は負荷分散装置のあるファームウェア処理に原因があることをほぼ特定し、再起動により回復することが見込まれた。しかし、この負荷分散装置は仮想化され、複数の利用者用にそれぞれ論理区画が設定されていた。そして、A 社の論理区画を再起動した場合の共同利用している他企業 D 社のオンライン業務に影響する可能性を明確に排除できなかった。よって、A 社の判断により、D 社のオンライン業務が終了する時間まで障害対処を見送ることとなった。また、これらの状況は D 社には全く伝えられていなかった。

原因

直接の原因は、C 社製負荷分散装置の sod プロセスのメモリ資源が時間とともに増加するという既知の不具合であった。

単なる負荷分散装置の障害にも関わらず、その解決と業務の再開に多大の時間を要し丸一日間オンラインサービスが停止することとなった原因は、以下のとおりである。

- 負荷分散装置は D 社と共用しており、再起動等の対処による D 社サービスへの影響が不明のため、A 社の了解のもと対処を業務終了後まで先送りすることとした。

根本原因は以下のとおりである。

B 社においては、共同利用サービスで使用する負荷分散装置等の共用機器に障害が発生した場合の復旧について、利用者への影響範囲の明確化を含めた手順が整備されていなかった。また、利用者との間でも、障害復旧に関する合意ができていなかった。したがって、D 社に連絡するとともに A 社の論理区画を再起動するという、迅速な復旧のための対処が出来なかった。

一方、A 社は、障害発生時には、システムを D 社と共同利用していることは認識していたが、トラブル発生時等の情報共有のための利用者間の連絡体制は確立されていなかった。

対策

対策は以下である。

再発防止策）

- 障害復旧時の関係者（サービスの共同利用者であるA社とD社、事業者であるB社）の役割分担や、システムにおけるコンポーネント（各種機器（ハード・ソフト）、データ）ごとの回復措置の利用者業務への影響範囲を明確化する（表2.8－1）。特に、障害発生時に停止／再起動する単位と、その停止により影響を受ける利用者の範囲を事前に整理・明確化する。
- B社は、システムを停止／再起動させる場合についての条件や手順、責任等に関する取決めをSLAで定義し、共同利用各社と合意する。
- 共同利用者間の情報共有の強化を行う。基本的にこれはサービス事業者の役割であるが、共同利用サービスでは、共同利用者間の日常の情報共有を行うとともに、非常時の緊急連絡体制等を定めておくことが望ましい。

表2.8－1　コンポーネント（今回の事例）

ハードウェア	負荷分散装置、ネットワーク機器、サーバ（アプリケーション, DB, Web）
ミドルウェア	仮想化OS, ゲストOS, OLTP（オンライン基盤ソフトウェア）など
アプリケーション	業務アプリケーション
データ	データベース, 一般ファイル

効果

障害発生時に、障害対応と再起動のための他社のオンライン業務の一時停止の協力等が得られるので、早急なシステムの復旧と業務継続が可能となる。

教訓

共同利用システムでは、利用者は通常はシステムの内容は理解していないので、障害が発生してもサービス事業者に頼るしかない。しかし、障害により困るのは業務サービスを利用するサービス利用者、エンドユーザなので、もしもの場合に備え、影響範囲等の制約条件を含む障害復旧手順を明確にするとともに、共同利用者間での情報共有を図ることが必要である。