3.17 定期的な再起動に関する教訓（T17）

教訓 T17

長時間連続運転による不安定動作発生の回避には定期的な再起動も有効！

問題

教訓 T16 と同じ事例である。特記事項としては、A 社のシステムでは、本稼働以来、負荷分散装置は 8 カ月以上連続運転状態であり、一般的なネットワーク機器と同様に再起動をしたことがなかった。

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。本不具合に関する技術情報とファームウェアの修正パッチは、A 社のシステム障害が発生する約 1 カ月前に、C 社より公表されていた。

根本原因は以下である。

負荷分散装置の再起動によりこの不具合による障害発生を回避することが可能であった。

しかし、A 社のシステムでは、本稼働以来、負荷分散装置は 8 カ月以上連続運転状態であり、一般的なネットワーク機器と同様に再起動をしたことがなかった。

今回の障害は定期的に再起動をしていれば顕在化しなかった。

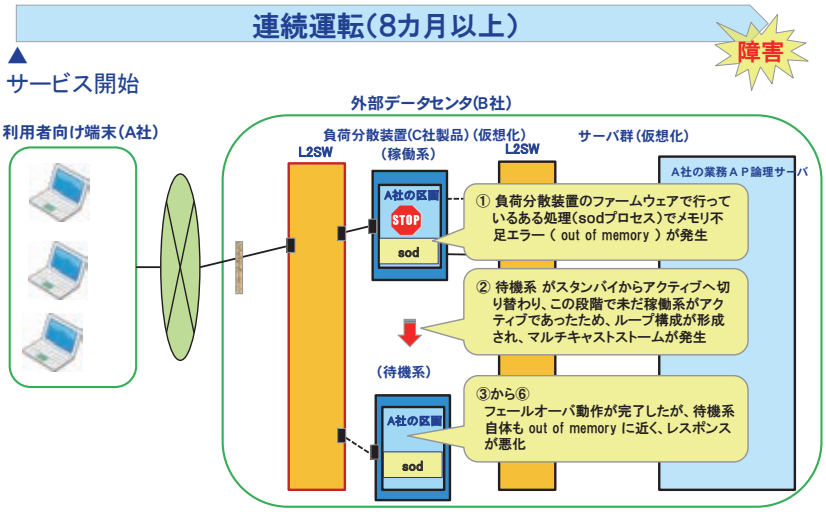

図 3.17－1　障害の経緯

対策

原因となった不具合は、装置の再起動により障害発生を抑止できるものであったため、直接対策としては、まず、負荷分散装置を再起動した。

その後、期間をおいて負荷分散装置における既知の不具合に関する技術情報を確認の上、業務への影響が少ないタイミングでその修正パッチを適用した。

再発防止策としては、本来の対応として、装置に関する技術情報をこまめに確認するルールを設けた。

さらに次善の対応として、システムの再起動のサイクルを検討し、定期的な再起動も行うこととした。具体的には、保守ベンダ（B 社）と協議して、毎月の定期保守日に状況を見て再起動を行うこととした。

効果

ネットワーク機器を定期的に再起動することにより、長時間連続運転による不具合の顕在化が回避でき、障害発生のリスクを低減できる。

教訓

ネットワーク機器については、定期的に再起動することにより、長時間連続運転による不具合の顕在化が回避できることが経験的に知られている。

かつては単純な機能がハードウェア制御により実現されていたため、可用性向上等のために連続稼働されていたが、近年では複雑な機能がファームウェア／ソフトウェアにより実現されているものが出現してきている。そのため、潜在的な不具合によるシステム障害発生のリスク低減のために、サービスに影響のないタイミングで定期的に再起動することも有効である。