3.16 修正パッチの適用に関する教訓（T16）

教訓 T16　システム構成機器の修正パッチ情報の収集は頻繁に行い、緊急性に応じて計画的に対応すべし

問題

A 社はオンラインによる情報登録及び情報照会の基幹業務システムを当初はオンプレミスで運用していたが、運用コストの削減を目的に複数企業間の共同利用を進める方針となり、B 社が提供するデータセンターに移行した。B 社が提供するシステムは、業務システム用のサーバと負荷分散装置に分かれている。業務システムのサーバだけでなく、負荷分散装置も仮想化されており、その一つの論理区画を A 社は利用していた。ある日、オンライン開始時からこのシステムに障害が発生してまる1日業務が停止した。基幹オンラインシステムが端末から起動できず、すべての窓口でデータベースの更新をともなう処理の受付けができなかった。

システムが障害となった経緯は以下の通りである。（図 3.16－1）

① 負荷分散装置のファームウェアで行っているある処理（sod プロセス）にてメモリ不足エラー（out of memory）が発生した。

② 待機系がスタンバイからアクティブへ切り替わり、この段階で未だ稼働系がアクティブであったため、両系間で多数の電文が繰り返し転送される現象（系間ループ形成によるマルチキャストストーム）が発生した。

③ L2 スイッチのポートが閉塞した。

④ sod プロセスが再起動された。

⑤ 稼働系がスタンバイへ切り替わった。

⑥ 系切替え（フェールオーバ）動作が完了し、待機系に切り替わったが、待機系自体が out of memory に近い状態であったため、極端なレスポンス悪化が発生した。

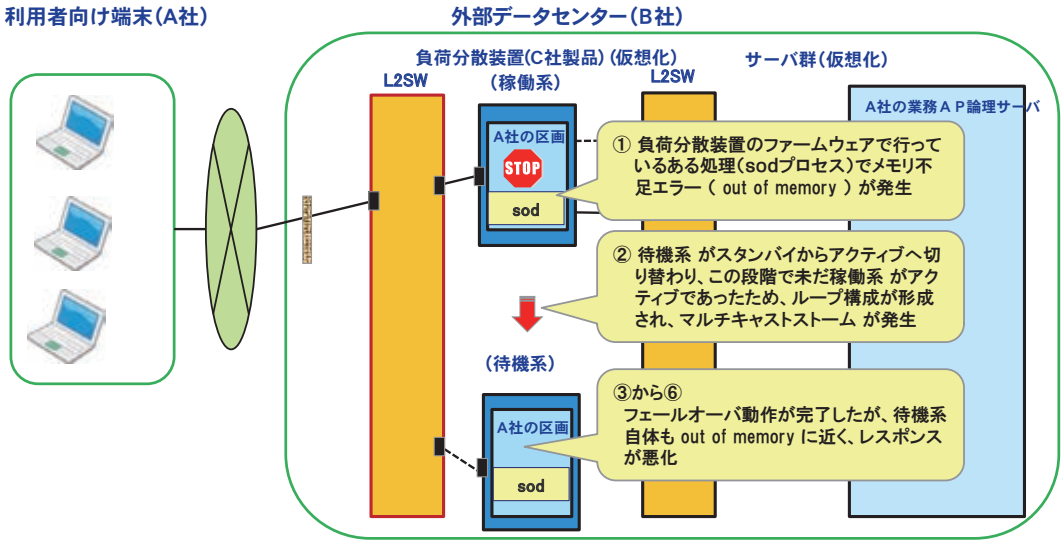

図 3.16－1　障害の経緯

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。

B 社は、システム構成機器の技術情報の確認サイクルを、3 カ月に 1 回程度と非常に粗く設定していた。そのため、パッチの公表に気づかず、本障害発生前に出ていた負荷分散装置の重大障害の修正パッチを適用できなかった。また、A 社は、同社のシステムを構成する負荷分散装置に関する技術情報が、メーカより時々公表されていることを認識していなかった。

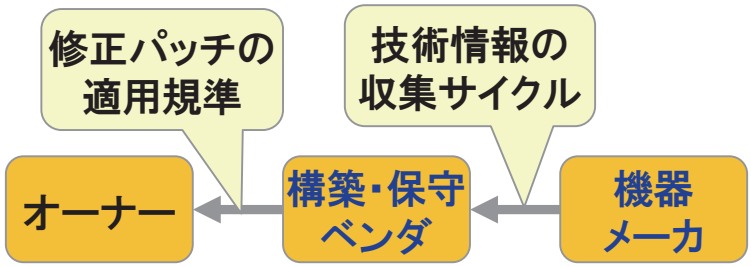

図 3.16－2　パッチ適用の流れ

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、A 社と B 社とで協議の上、技術情報の確認サイクルを見直して 3 カ月に 1 回から 2 週間に 1 回に変更した。特に重大な不具合では、修正を反映させる手立てや修正の優先度付けを行うこととした。

効果

構成機器の技術情報の収集に漏れがなくなり、障害発生が予防できる。

教訓

ネットワーク機器についても、修正パッチ情報等の技術情報を定期的に検索し、その緊急性に応じてパッチを当てるか否か判断する。また、特に重大な不具合では、修正を反映させる手立てや修正の優先度付けが重要である 。

特に、クラウドサービスなどでは、パッチの適用については、オンプレミスと異なり、利用者には、自らパッチの情報を得て適用する方策がないため、パッチ情報の提供者（サービスやハード・ソフトを提供する側）とパッチの適用判断者（主にサービスやハード・ソフトを所有する側）がお互いに協力しあうことが信頼性の向上につながると考える。