２．７　クラウドサービス利用時の障害対応体制に関する教訓（Ｇ７）

[教訓 G7]
クラウド事業者と利用者が連携した統制がとれたトラブル対応体制を整備すべし

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 社が提供するクラウドサービスに移行した。同時期に共同利用に移行するのは他に D 社があり、類似のビジネスを行っていた。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。（図２．７－１システム概要）

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伴う処理の受付けができなかった（①）。

なお、A 社があらかじめ用意していたクラウド外の「障害時バックアップシステム」に切り替わり、データ照会処理はできたので、データの更新を伴わないサービスのみを実施した（②）。

B 社は障害箇所の特定に時間を要し、またＡ社は各方面への説明対応に追われたこともあり、障害箇所が判明したのは１６：００であった。すでに業務終了時間が近づいていたためオンラインは終日停止、障害復旧作業はその後実施となった。

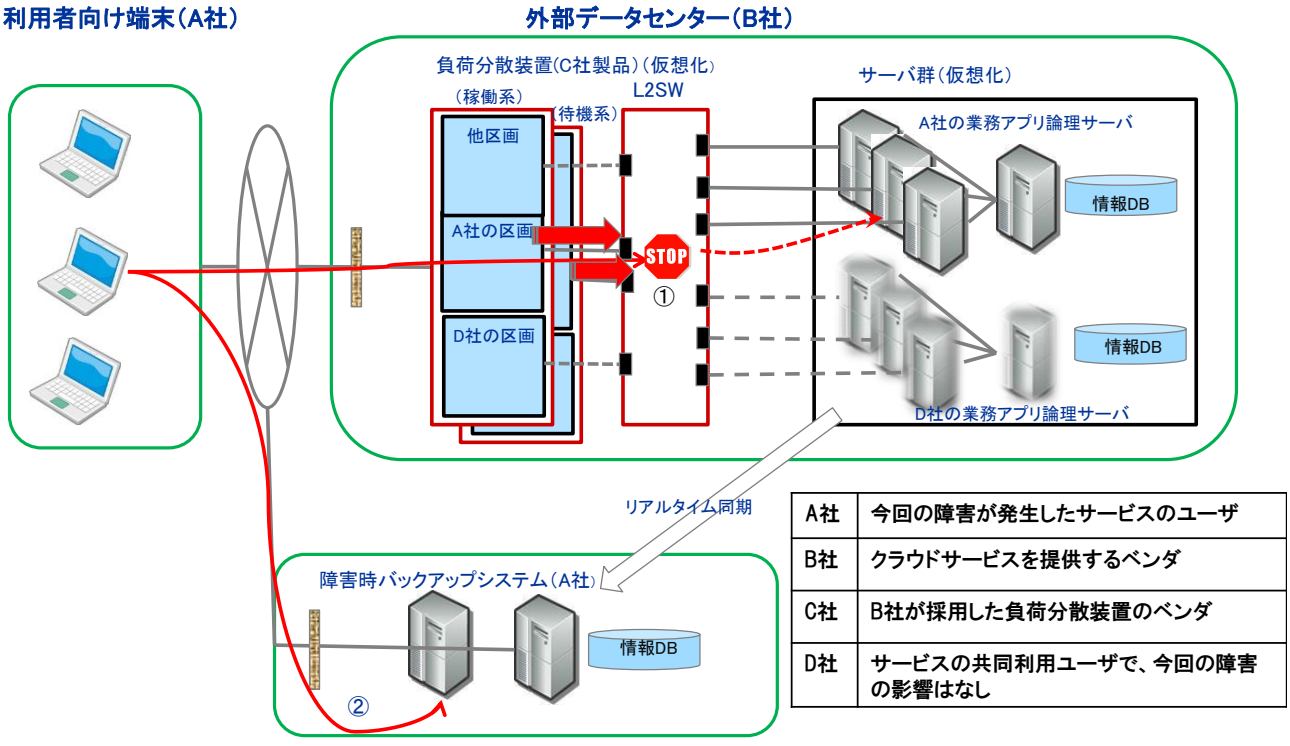

図２．７－１システム概要

原因

直接の原因は、C 社製負荷分散装置の sod プロセスのメモリー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。

・通信路の疎通状況を確認する ping が通ったことから、B 社はシステムの運用に問題ないと誤認した。
・初めのうちは AP サーバや専用線の問題と誤認し調査を行っていた。B 社の自社製品ではない C 社製負荷分散装置の障害調査は後回しにした。
・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。

１．運用時のトラブル管理体制が決まっていなかった。
・障害調査を進め、一体となって協力して進めていく体制ができていなかった。B 社の SE は A 社に常駐していたが、トラブル管理体制が明確化されていないので、報告、連絡、相談がうまく回らなかった。
２．A 社は B 社と役割分担やサービスレベルが不明確な運用委託契約のままサービスを開始していた。
３．B 社に C 社製負荷分散装置の専門家が不在で、社外の製品のため障害情報の入手もしづらく、障害やパッチの情報をタイムリーに入手していなかった。

対策

再発防止策は以下のとおりである。

１．トラブル対応の体制の強化
トラブル管理体制を明確化し障害発生時の報告、連絡、相談を行う。
（考慮すべきこととして、ユーザーは、対応をベンダー任せにせず積極的に働きかける。
ベンダーは、ユーザーに対する状況報告を密に行う）
トラブル発生時はユーザーとベンダーを TV 会議で結び、ユーザーとベンダーが密接に協力して対応するなどを検討する。
２． 適切な契約でサービスのレベルの定義を行い、責任分界点を明確にする。
３．ベンダーは関係する各サードパーティ業者とトラブル対応体制を確立し、障害時の連携を適確に行う

効果

クラウドサービスにおいても役割や責任が明確となり、障害発生時のエスカレーションや対応を迅速に行うことができる。

教訓

ユーザーはクラウド型システムの障害発生に備えて、クラウド事業者と連携した統制がとれたトラブル対応体制の整備が必要である。特にユーザーはベンダーに対して、役割分担や契約などのやるべきことをはっきりと要求し、厳しく緊張感を持って対応すべきである。これによりシステムの信頼性が向上するだけでなく、両者がお互いに成長することができる。

参考資料)

クラウド適用のガイドラインについて (http://www.aspicjapan.org/guideline/index.html)