要旨

１．はじめに（クラウドの普及状況）

近年クラウド化の進行は著しく、総務省の調べ（※１）では２０１６年１２月時点で企業の４６．９%が利用しているとの結果が出ていた。

クラウドサービスは自社でサーバを設置するよりも初期費用が安く、短期間での導入が可能。また必要な分だけ購入が出来る等メリットが多い。一方デメリットとしては、カスタマイズの制限やブラックボックスなセキュリティへの不安が挙げられることが多いが、それらと並んでサービスの継続性を懸念する声もある。

もし利用中のクラウドが突然サービスの提供を停止したら・・・場合によっては甚大な被害が発生することになる。その被害を増大させる原因となるものが「ベンダーロックイン」である。

本研究では、クラウドにおけるベンダーロックインについて、脅威の分析を行い、回避策の検討とその効果について考察を行った。

２．ベンダーロックインとは

特定ベンダー（メーカー）の独自技術で作られたサービス、システム等を利用した際に、他ベンダーの提供する同種のサービスへ乗り換えが困難になる現象のことだ。

今よりも良いサービスを使いたいと考えた時に他社の製品へ切り替えが難しく、価格が高騰しても同じサービスを使い続ける選択肢しかなくコストが増大するケースが多い。また、市場の競争による恩恵を十分に受けられない可能性もある。

ベンダーロックインには「コーポレートロックイン」と「テクノロジーロックイン」の２種類がある。システムを同じベンダーから調達せざるを得なくなる現象を「コーポレートロックイン」と言う。それに対し、「テクノロジーロックイン」はある製品や技術の独特な開発手法を使うことにより他の製品への移行が困難になる状況のことを言う。

３．調査

今回ターゲットにしているクラウドでは主に「テクノロジーロックイン」が生じる。また、ロックインによる最も警戒すべき脅威としては、利用料の急激な値上がりや利用中のサービス停止が挙げられる。クラウドサービスという特性上、利用料やサービスの継続は全てクラウドベンダーに委ねられており、ユーザ側ではコントロールが出来ないからだ。これらの脅威が実際に発生した場合、コストの増大、移行作業の長期化による事業の中断、といった被害が想定される。

クラウドはＩａａＳ・ＰａａＳ・ＳａａＳと大きく分類することが出来る。そこで、それぞれロックインされるとどのような違いがあるか調査を行った。ＩａａＳでは既にコモディティ化が進んでおり、価格競争が繰り広げられているため独自機能は少ない。

要旨

一方でＰａａＳ・ＳａａＳは機能の差別化で各社が競っているため、独自機能が多くなる。つまり、ＰａａＳ・ＳａａＳを利用するとロックインされるリスクが増すことになる。

４．回避策と効果

クラウドロックインの回避策として、「マルチクラウド」と「標準化された技術」の活用が効果的ではないかと考えた。

１）マルチクラウドでリスク分散

複数のクラウドサービスを組み合わせることでリスクが生じた場合他のクラウドに切り替えることが容易になる。

２）標準化された技術の活用

クラウド独自のサービスは使用せず、環境に依存しないシステム構築を行うことで特定のクラウドへのロックインが回避される。

マルチクラウドで効果シミュレーションを行った結果、以下のことが分かった。

・機能分散型のマルチクラウドは被害を軽減することができる

・冗長化によるマルチクラウド構成はロックイン対策としては有効ではない

（突然の大規模障害対策向き）

５．まとめ

クラウドロックインの回避策を講じると初期構築の費用や運用負荷が余計にかかり、クラウドのメリットであるコスト削減と俊敏性が活かせなくなる。従って、全てのケースにおいてロックイン回避すべき、という結論は出せなかった。

システムライフサイクルや技術革新の早さなどのシステムの特性を考慮してクラウドロックインを回避するか､反対に自らロックインされクラウドの恩恵を最大限受けるか、戦略を定めることが重要である。

以上

出典

※１：総務省ホームページ

http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc262140.html