

新たなITリスクに立ち向かう 連載シリーズ 第2回 クラウドサービスの活用

インターネット技術の進歩、ITコストの削減要請、経営スピードの変化、国際化を背景に、「安く、早く」導入できるクラウドコンピューティングの活用が叫ばれて久しい。IT関連の記事・雑誌で「クラウド」の文字を見ない日はほとんどなく、近年はバズワード¹化している感がある。

経営におけるシステムの重要性は年々高まりつつあるが、特に「他社と差別化することに大きな重要性がないシステム」において、「安く、早く」導入できるクラウドサービスは経営者のニーズにマッチしており非常に魅力的である。

一方で、クラウドサービスは、自社だけの意思で統制できない情報セキュリティ管理や、契約の司法権が日本に限らない等、日本における従来型のシステム開発・運用における外部委託とは異なる性質のリスクを多く有している。

本稿では、「新たなITリスクに立ち向かう」の第2回目テーマとして、「クラウドサービスの活用」について述べていきたい。

1. クラウドサービスの本質とは

クラウドサービスの本質を理解するにあたり、特に押さえておきたいポイントは以下の3点と考える。

(1) コスト低減のメカニズム

クラウドサービスのコスト低減効果は、クラウド事業者がクラウド利用者に共通のITリソースを提供し、サービス利用者がITリソースを効率的に利用することを通じて生み出されている。お互い顔を知らない利用者同士が、ネットワーク上のITサービスを共有し、使用量に応じたコストを負担する仕組みである。

一方、情報セキュリティ対策など、各ユーザーが共通的に望むと想定される機能については、各クラウド事業者の判断で投資の必要性について意思決定が行われるため、自社固有の要求を提示する場合には、相応のコスト負担を追加的に要求されることもある。

これらのことから、サービス利用者は個別要望を極力減らし、事業者によって共通化されたサービスレベルを受け入れることが、コスト削減メリットを享受するための重要なポイントとなる。



1 バズワード：一見、説得力があるように見えるが、具体性がなく 明確な合意や定義のないキーワード

(2) サービスの継続性

クラウド事業者にとって当サービスは慈善事業ではなく、ビジネスとして採算を確保しなければならない。すなわち、サービス継続の観点から一定の収益を上げることがクラウド事業者にとって最大の関心事であり、極端に言えばシステムがどの程度利用者にとって重要か、どのようにシステムを利用しているかはクラウドサービスの継続性と関係がない。したがって、クラウドサービスの採算が悪化した場合、ある日突然サービスが停止するというリスクが存在する。

実際に、米国では昨年10月にクラウドストレージサービス大手のNirvanix社が破産し、大混乱を招いた事例も発生しており、サービス利用者は、サービス事業者の経営状況、クラウドビジネスの採算に常に関心をもつことがサービス継続性を担保する上で重要なポイントとなる。

(3) ボーダーレス化

クラウドサービスには国境が存在しない。海外のクラウドサービスを利用する場合、サーバ設置場所(国)が公開されないケースもあり、紛争時にどこの国の法律が適用されるのかという不安や、海外政府に自社データを監視されているのではないかとといった不安がつきまとう。実際、NSA(米国国家安全保障局)によるインターネット／電話回線の傍受が暴露されたことは記憶に新しい。

また、海外ベンダーが提供しているクラウドサービスでは、サービス事業者の本社所在地やサーバ所在国の法律が適用されることが多く、サービス利用者は海外の法律を意識して契約を締結しなければならない点について、特に留意しなければならない。

2. クラウドサービスの主要リスク

クラウドサービスに関するリスクを網羅的に表現した基準としては、欧州で発行されたENISA(欧州ネットワーク情報セキュリティ庁)の基準が有名であり、リスク種類を35種類に分類している(表1参照)。本稿では、特に重要で論点となる3つのリスクを紹介する。

(1) 情報セキュリティリスク

クラウドサービス導入に関し、利用者が最も不安に感じるリスクの代表格が情報セキュリティに関するリスクである。

自社でシステムを開発・運用している会社は自社が期待するセキュリティ水準を決定することができ、外部委託する場合は自社の要求水準を満たす委託先を選定し、必要に応じ直接モニタリングを行い、改善を促すことが一般的である。

一方、クラウドサービスを導入する場合は、自社のみの都合でクラウド事業者のセキュリティ水準を要求・決定することはできない。クラウドサービス事業の根幹となるコスト低減要求と利用者からのセキュリティ強化要求で利害が相反する局面が存在し、サービス導入に二の足を踏む企業が多い。金融機関等規制当局の監督下にある業界では、クラウドサービスに関して当局の関心も高いため、特にその傾向が顕著である。

(2) クラウドサービス終了リスク

クラウドサービスは、サービスにより一定の利益が出ない場合に事業者側に積極的に継続するインセンティブは存在しない。サービス事業者にとってサービスの終了は評判リスクに直結するので非常に重い決断となるが、特に海外のクラウドベンダーは本国の方針で突然サービスが停止してしまうリスクがゼロではないと考えられる。たとえば、米国系クラウドサービス事業者も日本に参入しサービスを展開しているが、「収益が出ないので、クラウドサービスは撤退」というシナリオは決して非現実的ではない。

(3) 法的リスク

海外にサーバを設置するクラウドサービスや、海外に本社のある企業とクラウドサービス導入の契約を締結する場合、司法権の異なる海外の法律の適用を受ける点について大きなリスク要因となる可能性がある。

たとえば、米国では司法がe-discovery法に基づき証拠提出命令を出すことがあり、命令を受けた他社とデータベース・ディスクを共有していた場合、自社機密データを含むハードディスクごと当局に没収されてしまうこともありうる。

【図表1】クラウドサービスのリスク

No	分類	項目
R1	ポリシーと組織関連 のリスク	ロックイン(サービスを移行しにくくなる等)
R2		ガバナンスの喪失(制御が及ばなくなる等)
R3		コンプライアンスの課題(関連要件への適用を確認出来ない等)
R4		他の共同利用者の行為による信頼の喪失
R5		クラウドサービスの終了または障害
R6		クラウドプロバイダの買収(サービス内容の変更等)
R7		サプライチェーンにおける障害(プロバイダの委託先からの影響等)
R8	技術関連のリスク	リソースの枯渇(リソース割当の過不足)
R9		隔離の失敗(適切なリソースの分離が行われない)
R10		クラウドプロバイダ従事者の不正・特権の悪用
R11		管理用インターフェースの悪用(操作、インフラストラクチャアクセス)
R12		データ転送途上における攻撃
R13		データ漏えい(アップロード時、ダウンロード時、クラウド間転送)
R14		セキュリティが確保されていない、または不完全なデータ削除
R15		DDoS攻撃(分散サービス運用妨害攻撃)
R16		EDoS攻撃(経済的な損失を狙ったサービス運用妨害攻撃)
R17		暗号鍵の喪失(暗号鍵やパスワードの紛失等)
R18		不正な探査またはスキャンの実施
R19		サービスエンジンの侵害(管理中枢機能の不具合等)
R20		利用者側の強化手順と、クラウド環境との間に生じる矛盾
R21	法的なリスク	証拠提出命令と電子的証拠開示(捜査による没収等)
R22		司法権の違いから来るリスク(国外の法律の影響を受ける等)
R23		データ保護に関するリスク
R24		ライセンスに関するリスク(ソフトウェアの利用形態が適用しない等)
R25	クラウドに特化しない リスク	ネットワークの途絶
R26		ネットワークの管理(ネットワークの混雑、接続ミス、最適でない使用)
R27		ネットワークトラフィックの改変
R28		特権の(勝手な)拡大
R29		ソーシャルエンジニアリング攻撃(なりすまし)
R30		運用ログの喪失または改ざん
R31		セキュリティログの喪失または改ざん(フォレンジック捜査の操作)
R32		バックアップの喪失、盗難
R33		構内への無権限アクセス(装置その他の設備への物理的アクセスを含む)
R34		コンピュータ設備の盗難
R35		自然災害

出典:「クラウドコンピューティング 情報セキュリティに関わる利点、リスクおよび推奨事項」 欧州ネットワーク情報セキュリティ庁(ENISA)、独立行政法人 情報処理推進機構(IPA) 翻訳(2009年11月)を基に筆者作成

3. クラウドサービス導入時におけるリスクへの対策

クラウドサービス導入におけるリスクへの対策は外部委託の対策と類似するが、大きく以下3点に集約される。

(1) サービス導入前のデューデリジェンス

クラウドサービスは、「利用者同士で機能を共通化することでコストメリットを享受する」サービスであり、導入前に期待した機能やサービス水準が実際とは違っていただけの場合に後からの変更は相当困難である。したがって、クラウドサービスを導入する場合は必要機能の有無、期待する情報セキュリティの統制・サービスレベル水準、事業者の財務状況、クラウドサービスの戦略性について、通常の外部委託を上回る慎重さをもって、適正評価（デューデリジェンス）を実施することが重要である。

(2) 適切なSLAの締結

クラウド事業者は、前記したクラウドのリスクについて、「自社のサービスは大丈夫です、安心です」といった営業資料・パンフレット・自己評価シート等を利用者に提供し、契約を獲得するための努力を怠らない。しかしながら、それらは口約束や営業トークと同様であり、法的効力が弱い。

特に海外のクラウドサービスを利用する場合や、会社にとって重要なシステムをクラウド化する場合、サービスレベルを細かく規定した契約書（SLA: Service Level Agreement）を必ず締結することをお勧めする。事業者が提供するSLAの雛形は一般的には、事業者側のリスクが最小化されるように策定されているため、修正せずに雛形のまま受け入れて締結することは、リスク管理上、問題があると考えられる。

(3) 継続的なモニタリング

会社の統制環境、経営環境、外部環境は常に変化するものであり、(1)で実施したデューデリジェンスの結果は、当然ながらその状態が未来永劫続くことを保証していない。したがって、クラウドサービス導入後は、通常の外部委託同様、継続的にモニタリングすることが重要となる。複数利用者が同時に利用するクラウドサービスの性質から、サービス利用者が直接サービス事業者を訪問し統制状況をチェックすることは現実的ではなく、サービス事業者が依頼した第三者機関による監査報告書を定期的に入手・確認するという方法が最も一般的である。

クラウドサービスの主要リスクに対する対策について、一般の外部委託と比較した結果を次頁の図表2にまとめたので、ご参照いただきたい。

【図表2】クラウドサービスの主要リスクと対策に係る論点（国内外委託との比較）

対策 主要リスク	サービス導入前の デューデリジェンス	適切なSLAの締結	継続的なモニタリング
情報セキュリティ リスク	評価すべき内容はほぼ同じであるが、サービス導入後の要求水準の調整は難しいため、外部委託と比較し更に慎重な評価が要求される。	サービス導入後のセキュリティ水準の個別調整が外部委託に比べ難しいため、より細かくセキュリティ水準を契約に規定する必要がある。	モニタリングすべき内容はほぼ同じであるが、クラウドの場合は1つのサービスに複数の利用者が存在するため、事業者側が提供する第三者機関の監査報告書を定期的に検証する方法が主となる。
クラウドサービス 終了リスク	外部委託と比較し、クラウドサービスが終了した場合、他サービスへの移行に一定の時間を要するため、サービス事業者の経営状況／業界内の評判を慎重に評価する必要がある。	サービス終了時の事前通知期間をできるだけ長く設け、M&Aの被買収時に契約が有効に存続する条項を盛り込む等、より保守的な契約に規定する必要がある。	サービス事業者の経営状況、業界内での評判に常に留意すること、特に海外のクラウド事業者は日本撤退リスクが大きいことを考慮し、サービス継続性を評価する必要がある。
法的リスク	海外に本社のあるクラウド事業者を利用する場合や、海外にサーバを設置する場合、紛争時にどこの国の法律が適用されるかを把握し、慎重に評価する必要がある。	海外の法律が適用される場合、日本では想定していないリスクが存在することがあるため、弁護士や外部専門家との連携をより密接に行ない、締結内容を規定する必要がある。	法律が適用される国の法制度・ガイドラインの変化を常にモニタリングし、新たなリスクが発生していないかを継続的にモニタリングする必要がある。

4. まとめ

クラウドサービスは、一般的に「安く、早く」導入できるため経営上のメリットが大きいものの、一般的な外部委託とは性質の異なるリスクも存在し、より慎重かつ細心な対策が必要なのは間違いない。しかしながら、リスクの内容を正しく把握し、適切な対策を行うことでリスクを低減できれば、そのメリットを十分に享受することができるサービスである。

KPMGではクラウドサービス導入をサポートするために、以下のようなサービスを提供している。

- ・クラウド導入支援／診断サービス（利用者向け）
- ・クラウドSLA締結支援サービス（利用者向け）
- ・クラウドセキュリティ監査サービス 保証型（事業者向け）

自社のどのような業務・システムに適用すべきかを十分見極め、クラウドサービスの活用をご検討いただきたい。

KPMGビジネスアドバイザリー株式会社
ディレクター 原田 克樹

KPMGビジネスアドバイザリー株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番7号
大手町フィナンシャルシティ サウスタワー
TEL : 03-3548-5305
FAX : 03-3548-5306

名古屋事務所
〒451-6031
名古屋市中区牛島町6番1号 名古屋ルーセントタワー
TEL : 052-571-5485

www.kpmg.com/jp/ba

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供しよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

©2014 KPMG Business Advisory Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.