リスクマネジメント最前線
2012-14

東京海上日動火災保険株式会社
企業営業開発部
〒100-8050
東京都千代田区丸の内 1-2-1
TEL　03-5288-6589
FAX　03-5288-6590
http://www.tokiomarine-nichido.co.jp/
東京海上日動リスクコンサルティング株式会社
http://www.tokiorisk.co.jp/

災害対策としてのクラウドサービスの活用と IT リスク

6 月 20 日、レンタルサーバー事業者が提供するクラウドサービス[1]で大規模な障害があり、データが大量に消失する事故が発生した。専門業者による復旧作業が試みられたものの、最終的に 5,000 件以上の企業のデータが失われる事態となった。また、自社でデータのバックアップをとっていなかった企業が多かったことも被害を拡大する一因となった。この事故により、ウェブサイトやメールだけでなく顧客情報やスケジュールなどのデータも失い、一時的に業務停止を余儀なくされた企業もあった。

本稿では、近年注目を集めているクラウドサービスの活用を災害対策の観点から述べるとともに、クラウドサービスを利用する上でのリスクとその注意点について解説する。

1. クラウドサービスとは

近年、クラウドコンピューティングが注目を集めている。クラウドコンピューティングを上手に利用することで、従来よりも少ないコスト負担や人的資源でより高度な IT の活用ができると考えられている。特にこれまで負担を感じて IT の活用に十分に取り組めていなかった中小企業にとっては、ブレイクスルーになるとして期待されている。

クラウドコンピューティングとは、ネットワーク上のサーバーが提供するサービスをそれらのサーバーの性能や構成を意識することなく利用できるコンピューター環境を指すものであり、クラウドサービスとは、このクラウドコンピューティングに基づいて提供される IT サービスである。企業が個別にコンピューター環境やアプリケーションを所有して利用するのに比べて、IT 資源の調達や開発、運用・保守の負担が軽減され、コスト削減にもなる技術として注目されている。

なお冒頭に述べたレンタルサーバー事業者が提供していたサービスは、厳密にはクラウドサービスとは異なるものである[2]。しかし、当該事業者が自社のシステムをクラウドサービスと広告していたことなどもあり、報道等では今回の事故をクラウドサービスの障害事例として扱っていることが多い。本稿は同様な事態がクラウドサービスを利用する上でも起こり得ることから、今回の事故を踏まえて注意すべき点について述べるものであり、サービスの技術的な相違を論じるものではない。そのため、以下では当該事業者のサービスをクラウドサービスとして扱っている。

---

1 本稿において当該事業者のサービスを「クラウドサービス」として表記する点については後述する。

2 当該事業者のサービスは、1 台のサーバーを複数のユーザーで共有する「レンタルサーバーサービス」であったのに対して、「クラウドサービス」は 1 台のサーバーを複数のサーバーがあるように動作させる仮想化と呼ばれる技術によって実現されるものである。

前述のように、クラウドサービスではこれまでの「所有する IT」から、所有を前提としない「利用する IT」へと転換できることから、次のような利点があると考えられている（表 1）。

表 1　クラウドサービス活用の利点

IT の調達に関わるコスト負担の軽減	サーバーやアプリケーションの調達、設置・設定に伴う初期コストの負担が軽減される。 IT 設備やシステムの更新に伴う資本投下の負担が軽減される。
IT の運用・保守作業からの解放・負荷の軽減	システムの運転・定期点検、OS やアプリケーションのアップデート・トラブルシューティング・ライセンス管理作業から解放される。 社内ユーザーのサポートやベンダーとの連絡・折衝に伴う作業負荷が軽減される。
IT 資源利用の柔軟性・拡張性の獲得	処理量・利用量の増大に対応して柔軟な設備増強が可能となる。
セキュリティ対策負荷の軽減	不正アクセス監視の負荷が軽減される。 セキュリティの設定や変更、対策実施に伴う作業負荷が軽減される。

出典：独立行政法人情報処理推進機構『中小企業のためのクラウドサービス安全利用の手引き』(2011 年 4 月）を基に弊社作成

さらにこれらの高可用性（IT 設備やシステムが必要な時に利用できること）・高拡張性の実現やトータルコストの削減だけでなく、災害対策の観点からもクラウドサービスの活用が有効と考えられており、企業が事業継続を実現するための対策としても注目されている。

2. クラウドサービスの活用と懸念

（1）　災害対策としての活用

昨年の東日本大震災は国民の生活や地域の経済活動だけにとどまらず、企業の IT 戦略にも影響を与えることになった。

震災以前より、大企業を中心に多くの企業では自然災害やパンデミック（大規模な感染症の流行）への備えとして事業継続計画（BCP: Business Continuity Plan）の策定に取り組んでいた。ただし BCP は策定したもののその内容によっては莫大なコストがかかることがあるため、IT システムの災害対策にまで具体的に着手している企業は必ずしも多くなかった。その理由のひとつは、BCP をはじめとするリスクマネジメントは有事の際の備えといった意味合いの強い取り組みであり、多くの場合において投資対効果が早急に実現されるものでないことから、災害対策にどのタイミングでどこまで取り組めばよいのか判断が難しいことが挙げられる。しかし、東日本大震災を契機にして国内企業はその業種や規模によらず、本格的に災害対策を検討しなければならない状況に直面している。

震災を経験して、災害対策の緊急性も重要性も分かってはいるものの余力のない企業にとっ

て、初期投資や人的資源を抑えつつも早期の立ち上げと高い可用性を実現するクラウドサービスの活用は有効な選択肢であるといえる。震災によって企業では、「IT 資源の被災・データ消失」「多数社員の出社困難」「計画停電によるシステムダウン」などの課題に直面することとなったが、これらはいずれもクラウドサービスを活用することが解決策のひとつとなる。

① IT 資源の被災・データ消失

被災した企業が行わなければならない事業継続上の対応は、被害を受けた経営資源の復旧と重要事業の継続・再開であるが、IT 資源やデータについては、クラウドサービスを利用することで事業中断の懸念を最小限に抑えるとともに、速やかに元通りの事業環境へと復旧を図ることが可能となる。

② 多数社員の出社困難

東日本大震災では交通機関の停止や計画停電が実施されるなど、首都圏においても大きな混乱があった。出社できない社員が続出したために、業務を停止せざるを得なかった企業も見られた。この教訓から、社員が自宅からでも社内システムにアクセスできる在宅勤務環境を実現するクラウドサービスが注目を集めた。これまで在宅勤務制度と言えば業務効率化を図る目的で利用されている傾向にあったが、災害やパンデミックなどの非常時でも事業継続を実現する対策の一環として整備する流れに変わりつつある。

③ 計画停電によるシステムダウン

震災後の計画停電により、自社屋内で運用している情報システムはすべて利用できなくなる事態に直面した。そのため社員の在宅勤務環境を整備するだけでなく、サーバーなどの IT 機器についても社外に移そうという動きが続いている。その際、安定した電力供給が可能なデータセンターを利用したクラウドサービスが停電対策に有効な解決策として注目を集めた。

このように事業継続を推進するものとして、クラウドサービスを活用するメリットは多い。実際に災害対策の一環としてクラウドサービスに期待する声は少なくない。ある調査[3]では、導入費用が低減できる（74.2%）、運用・保守費用が低減できる（69.7%）などのほか、サービス継続性が高められる（30.4%）等の効果をクラウドサービスに期待している。

（２） クラウドサービス利用時の懸念

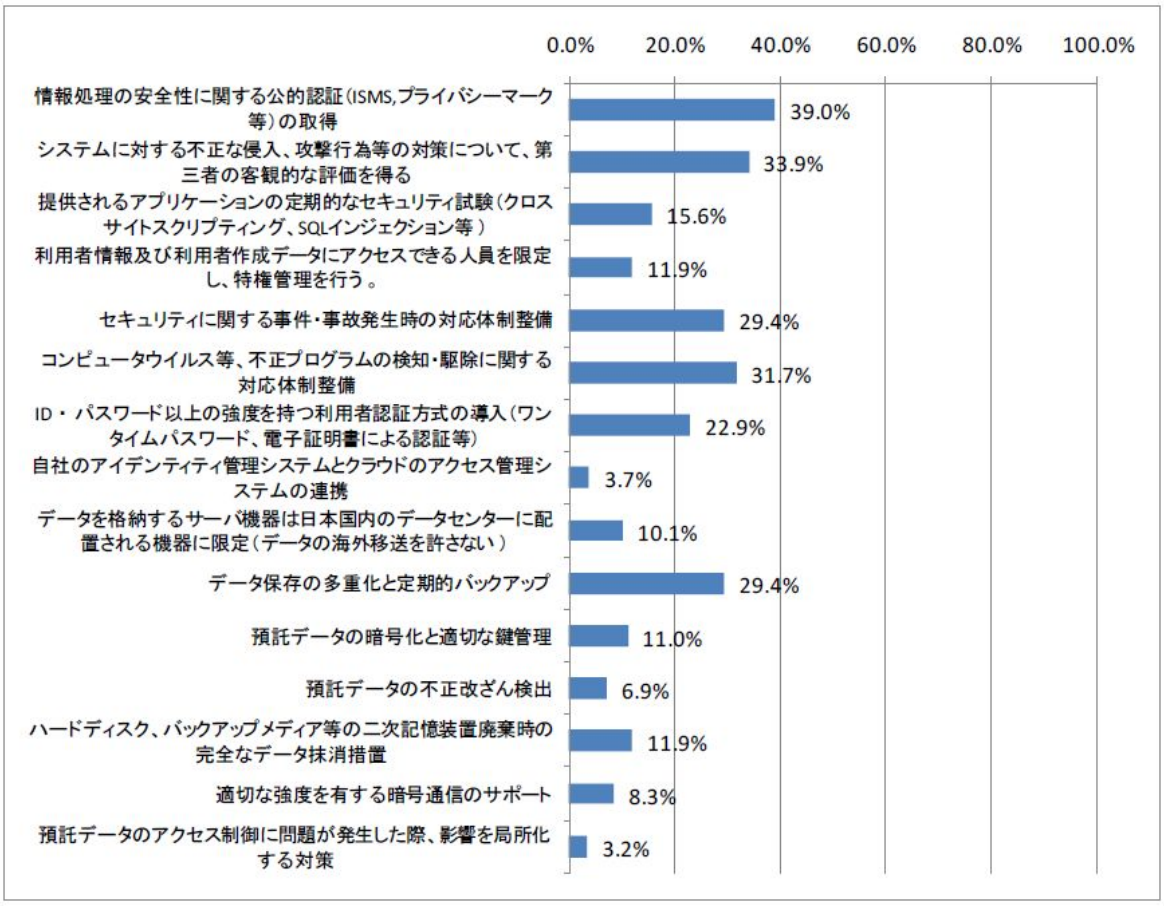
一方で、クラウドサービスを利用するにあたっていくつかの懸念が指摘されている。

中小企業等におけるクラウドの利用に関する実態調査[4]では、クラウド事業者が実施すべきセキュリティ対策として、「情報処理の安全性に関する公的認証の取得（39.0%）」「不正侵入・攻

3 独立行政法人情報処理推進機構『IT コーディネータが見た中小企業等におけるクラウドサービス利用上の課題・導入実態調査報告書』（2012 年 4 月）

4 独立行政法人情報処理推進機構『中小企業等におけるクラウドの利用に関する実態調査』（2011 年 3 月）

撃行為等の対策について第三者の客観的評価を得る（33.9%）」「コンピュータウイルス等、不正プログラムの検知・駆除に関する対応体制整備（31.7%）」「セキュリティに関する事件・事故発生時の対応体制整備（29.4%）」「データ保存の多重化と定期的バックアップ（29.4%）」などが上位に挙がっている（図 1）。



出典：独立行政法人情報処理推進機構『中小企業等におけるクラウドの利用に関する実態調査』（2011 年 3 月）

図 1　クラウド事業者が実施すべきセキュリティ対策

ユーザー企業とサービス事業者の橋渡しを担う IT コーディネータへの調査[5]でも、クラウドサービス導入時の課題・不安として、「自社の情報を他社に預けることに不安がある（データが壊れたり消えたりするかもしれない）」など、セキュリティに関する不安が 62.6%と最も高かった。

これらの懸念についてはクラウドサービス事業者の情報を総合的に判断し、リスクを見極め、また自らも十分な対策を施した上でサービスを利用する必要があることは言うまでもない。それでは、クラウドサービスを利用するにあたって、具体的にどのような点に注意する必要があるのかを以下に述べる。

5 独立行政法人情報処理推進機構　前掲注 3

３．クラウドサービスを利用する上での注意点

（１）　利用管理担当者の確保

今回の事故後、「クラウドサービスを利用する場合でも、企業は自らデータのバックアップを取るべきである」という意見が多かった一方で、「それではクラウドサービスを使うメリットが薄くなる」という声もあった。

有償のサービスを利用しているからといって自らのデータを守る責務からも解放されるわけではない。今回の事故でもバックアップデータさえ残っていれば、最悪の事態は防ぐことができた企業が多かったと推測される。クラウドだからといって安心せずに、バックアップを行なうことが必要であると改めて認識しなければならない。たとえサービス事業者がバックアップは不要といったことを宣伝していたとしても、自らでも最低限の対策は実施しておくべきである。

中小企業によるクラウドサービスの安全利用を目的に策定された独立行政法人情報処理推進機構（IPA）の『中小企業のためのクラウドサービス安全利用の手引き』(2011 年 4 月）でも、全ての管理をサービス事業者に任せるのではなく、企業自らが利用管理担当者を確保することを求めている。その上で担当者が、ユーザーアカウントの登録・抹消やサービス利用権限の管理、利用マニュアルの整備や利用方法の指導・ヘルプデスク、データの定期的なバックアップ、障害時のサービス事業者との連絡調整、処理量に応じたサービスの調整などを行うこととしている。

（２）　SLA の確認・見直し

一方で先にも述べたとおり、サービス事業者においてデータを安全に保管できていると確証が取れるのであれば、企業自らがバックアップしなくても良いとの判断もありうる。ただしその場合にはあらかじめ、サービス品質保証契約（SLA: Service Level Agreement）を確認することが不可欠である。今回のデータ消失事故では事故後に損害賠償請求が可能であるか議論となったが、一般的なクラウドサービスにおいて SLA ではデータの損失は免責事項であり、損害賠償の対象とはならない。クラウドサービスを利用するにあたっては SLA の内容をしっかりと精査し、トラブルが発生した際にどこまで責任を追及できるのかを確認した上で、バックアップの要否を含めた自らでの対策を判断するべきである。

（３）　サービス利用の意思決定

今回のような事故は決してクラウドサービスを利用した場合に限ったものではなく、同様の事態は社内システムのメンテナンスを外部の事業者に委託するような場合にも起こり得るものである。クラウドサービスの導入は企業の IT 戦略に係わる事案であるため、本来は新規システムの開発などと同様に経営トップや担当役員での判断が必要なものである。しかし、サービス利用時の申し込みの手軽さや費用面での心理的負担の低さもあり、その判断が現場の担当者任せとなっていた懸念がある。

前述の『中小企業のためのクラウドサービス安全利用の手引き』でも、クラウドサービスの利用範囲を検討し、取り扱う情報の管理レベルについて確認するとともに、「株式公開企業であるか」「事業を長年続けているか」「利用者は多いか」「事故の頻度は高くないか」「障害対応がきちんと行われているか」などといった項目によって、サービス事業者の信頼性を評価することを求めている。

システムやネットワーク構成、運用体制に懸念がないかをチェックするとともに、クラウドサービスに移行する業務範囲とそこで取り扱う情報の種類・範囲を決定する必要がある。

４．最後に

これまで述べたとおり、クラウドサービスでは IT 資源を所有しないことのメリットをリーズナブルな価格で実現できるサービスであるが、システムに対して自らの統制が及ばなくなるという潜在的なリスクが生じていることを認識する必要がある。

クラウドサービスを安全に活用するためには、サービスを利用することで生じる事態の責任は従来と変わらず利用者自身にあることを認識し、必要となる対策を講じることが求められる。

（2012 年 8 月 27 日発行）