2012.04

情報セキュリティニュース ＜2012 No.1＞

クラウド･コンピューティングにおけるセキュリティ上の課題と導入時の留意点

2011 年 3 月 11 日に発生した東日本大震災では、巨大津波とそれに続く計画停電等により情報セキュリティ上も大きな被害が生じ、クラウド･コンピューティング（以下クラウド）の役割の重要性が再認識された。被災地では多くの企業のみならず自治体においてもサーバが津波で流され、被災者支援上必要となる住民台帳データが消失、バックアップもなかったことから被災者の本人確認ができないなどの支障をきたした例も少なからず見られた。

その後、被災自治体や被災地･被災者支援を行う NPO 等に対して多くの大手 ICT 企業が無償でクラウドサービスを提供した。IPA（独立行政法人情報処理推進機構）の調査によれば、東日本大震災での緊急支援に役立てられたクラウド･サービスは 76 件にのぼる。その主たる用途は、安否確認、情報共有、行政情報発信、被災者支援の情報基盤の整備であった。この中には発災後わずか数日でサービスを立ち上げた例もいくつかある。提供期間については 3 ヶ月から 6 ヶ月程度のものが多いが、自治体向けには期限を定めていないものも少なくない。

このような対応事例から、地震などの大規模災害が発生した際のシステムの可用性確保やハードウェアが限定された環境下での迅速な情報インフラ確立の観点からクラウド･サービスが大きな役割を果たしたことがわかる。今後は政府、自治体や企業の災害時の事業継続の対策のひとつとして導入の検討が加速するであろう。

一方においては、企業のシステム担当者からは、クラウド導入にあたって、利点は理解しているものの、そのセキュリティ対策に懸念を抱くケースも少なくない。

そこで、本稿では、利用者側がクラウドについて懸念しているセキュリティ上の課題に焦点を絞り、最近の障害事例を紹介するとともに、導入に際しての留意点について解説する。

1. クラウドの特徴と市場規模

利用者としてのクラウドの利点としては、以下の点があげられる。

① 自前のコンピュータやハードウェア、ソフトウェア、設備などを保有、設計、開発、保守･管理する必要がなくなり、それに伴うコストが軽減できる。

② 利用者自身で購入した場合と比べると、陳腐化が避けられ、最新のアプリケーション･ソフトウェアが利用でき、財務上も資産の削減が見込まれる。

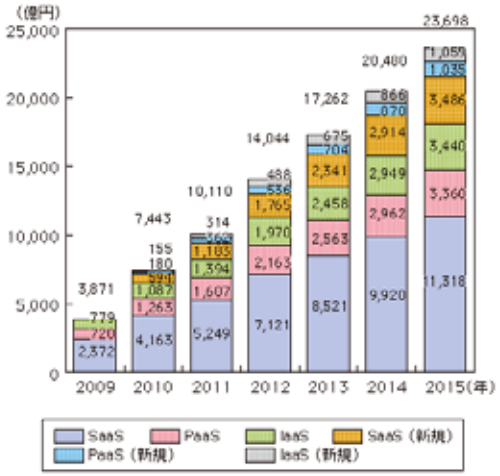
③ 利用者の事業規模や必要性に応じた、規模の拡大や縮小、サービス中断などが比較的容易に行うことが可能である。

④ 利用者がクラウド側にデータを保存する場合、利用者はネットワークに接続できる環境であればどこでも自社のデータにアクセスすることができる。

特に中小企業にとっては、コストを抑えながらも信頼性の高い最新サービスを利用できるメリットは大きい。

2010 年の総務省「スマート･クラウド研究会報告書」（次頁図1参照）によれば、クラウド･サービスの市場規模は、2009 年時点で約 3,900 億円と見込まれる。なかでも SaaS 市場の規模が大きく、市場全体の 61.3%を占めている。今後もクラウド･サービス市場は順調に拡大していくと見込まれ、2015 年には 2 兆円を超える市場規模になると推定される。

図1．クラウド・サービスの市場規模(推計)



SaaS：
アプリケーションやデータベースをサービスとして提供するクラウドサービス

PaaS：
オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス

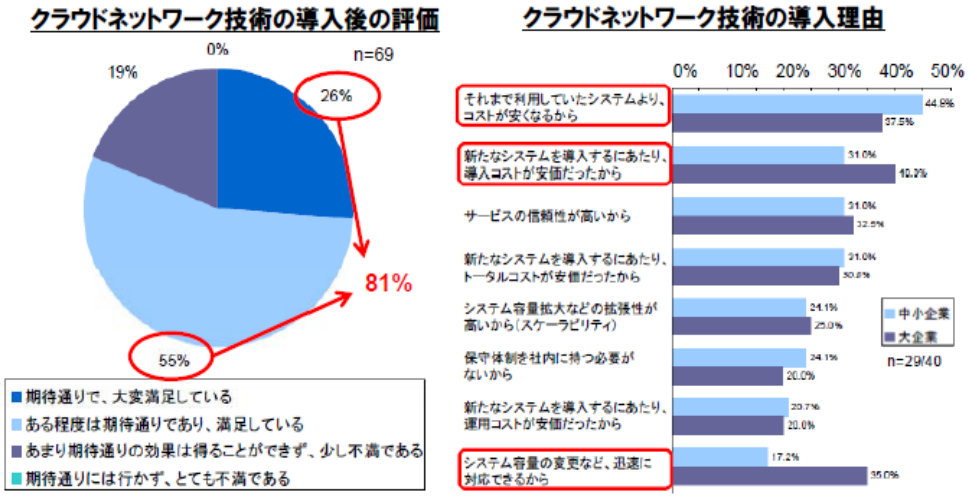
IaaS：
CPU、メモリ、ストレージ、ネットワークなどのハードウェア資産をサービスとして提供するクラウドサービス

(出典：総務省「スマート・クラウド研究会報告書」(2010))

2. クラウド・サービスに対する利用者の評価

2010 年の総務省の調査（下図2参照）によれば、クラウドを導入した企業のうち、約 81%が満足しており、とりわけ「コストの優位性」、「システムの容量変更における迅速性」、「サービスの信頼性」を高く評価している。

図2．クラウドネットワーク技術の導入後の評価および導入理由



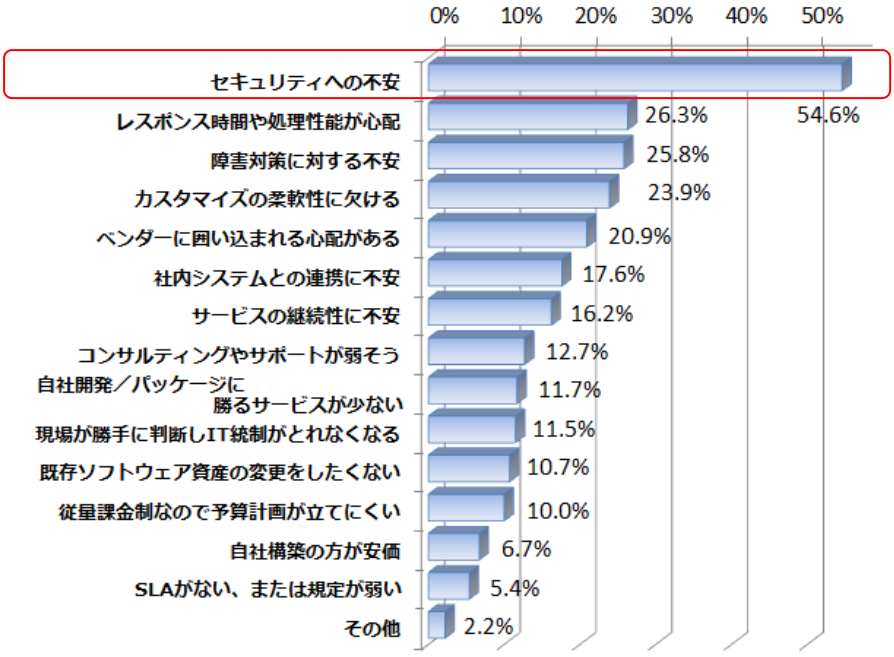
(出典：総務省「スマート・クラウド研究会報告書」(2010))

3. クラウド・サービスに対する利用者の懸念要因

上述の通り、多くの利点からその市場規模が急拡大しているクラウドではあるが、一方においては、そのセキュリティ上の課題が指摘されている。

IDC Japan が 2010 年 3 月～4 月に実施した調査（次頁図3参照）でも、回答者の 54.6%が「クラウドの最大の懸念事項はセキュリティ」と回答している。その他の懸念要因としては、レスポンス時間や処理性能、障害対策に関するものの割合が高い。

図3．クラウドサービスの阻害要因



（出典：IDC Japan「国内クラウドサービス市場ユーザー動向調査結果」（2010 年 6 月））

これらの懸念を受けて、クラウドのセキュリティに関する課題については、以前より論議されている。2009 年、NIST（米国国立標準技術研究所）、ENISA（欧州ネットワーク情報セキュリティ庁）、CSA（Cloud Security Alliance）等のクラウドのセキュリティに関する報告書が出された。一方、日本では、2011 年 4 月経済産業省の商務情報政策局・情報セキュリティ政策室より「クラウドサービス利用者のための情報セキュリティマネジメントガイドラインについて」が公表された。このガイドラインは 2010 年 10 月、ISO（国際標準化機構）/IEC（国際電気標準会議）に提案され、今後国際標準化の議論を進めていくことになっている。

4. 最近のクラウド・サービスの障害事例

以下にクラウド・サービスにおける最近の障害事例を挙げる。

① A 社のセキュリティ障害

2009 年 3 月、米インターネット大手 A 社が提供するオンライン上でドキュメントを作成・利用できるサービスにおいて、非公開のドキュメントが共有されてしまうという不具合が発生。利用者の 0.05%に影響。復旧まで数時間を要した。

② B 社へのゼロデイ攻撃（セキュリティの脆弱性の修正パッチが公表される前に悪用して行われる攻撃）

2009 年 6 月、英国の B 社の仮想マシンに対するゼロデイ攻撃によって、約 10 万件のウェブサイトのデータが喪失、顧客情報の流出も発生。

③ C 社のメール消失

2011 年 2 月、C 社の一部利用者のメールが消失。アップデートしたストレージソフトウェアのバグが原因。復旧に数日を要した。

④ D 社 のヴァーチャルマシンの大規模障害

2011 年 4 月、ストレージサービスのトラフィックを誤ってキャパシティの低いバックアップ用ネットワークに接続。復旧まで 10 日程度を要した。同サービスをインフラとして利用していた他の事業者のクラウド・サービスも停止。

⑤ E 社のクラウドサービスの停止

2011 年 5 月、E 社の仮想サーバサービスが接続不能になり、すべての仮想サーバが利用不能に陥る。原因はファイルシステムの不具合。復旧できず、サービス全体の提供を停止。

⑥ F 社のセキュリティ障害

2011 年 6 月、F 社のオンラインストレージサービスで約 4 時間パスワード機能に支障が発生し、任意のパスワードで他の利用者のアカウントにアクセスできる状態となった。

⑦ G 社のクラウド上の自治体向け電子サービスに対する DoS 攻撃

2011 年 11 月、G 社のクラウド上の自治体向けの電子申請システムが DoS 攻撃（ネットワーク機器に対して大量のアクセスを行うことにより一時的にサービス不能の状態にする攻撃）を受け、サービスが数時間停止。

5. クラウド・サービス導入の主なリスク

クラウド・サービス導入にあたって留意すべきクラウド固有のリスクには以下のようなものがある。

（1）契約・管理上のリスク

① 統制の喪失

- 機能の外部委託によりシステム全体を把握できない。また管理できない。
- 従来のサービスにおいては外部委託であっても、統制に必要な監査体制など整備できたが、クラウド・サービスではコントロールできない。

② 画一的な SLA（サービス・レベル・アグリーメント）

- 利用者と事業者間でサービスの品質の保証項目や障害の際の利用料減免を定めた SLA の条項が不十分な場合、トラブル発生時の対応が十分でなく、責任も不明確となる。
- 従来型のサービスにおいては、SLA の内容は利用者・事業者間で協議できた。一方、クラウド・サービスでは、SLA は画一的になり、この SLA に記載されていない事項は、原則的に利用者側の負担となる。

③ コンプライアンス規程との不整合

- 利用者側のセキュリティ運用方針と事業者側のセキュリティ用件が不一致となるケースが想定される。

④ 標準化、ガイドラインの未成熟

- 事業者側のストレージ、仮想化、相互運用性などの標準化が未発達な段階のものも少なくない。全体統治のガイドラインもない場合がある。
- 利用者側がクラウド利用時の自社の運用ガイドラインを策定しづらい。利用者が長い年月をかけて策定・改定してきた標準、ガイドラインが役に立たない。

⑤ セキュリティや品質のカスタマイズ化

- クライド化による一元管理が柔軟なカスタマイズを困難にしてします。

⑥ ベンダーロックイン（事業者が利用者を自社製品で囲い込むこと）

- アプリケーションの API（アプリケーションプログラムインターフェース）機能などが事業者の環境に依存するため、システムの移行性、可搬性を失う。
- 利用者は他社のクラウドサービスに移行しにくくなる。

（2）技術的なリスク

① ブラウザの脆弱性

- インターネット上でブラウザを介してサービスを利用する際に、ブラウザの脆弱性をついた攻撃を受ける危険性がある。（ブラウザの脆弱性は従来のウェブサービスでも存在したが、クラウドでは対象となるアプリケーションがより広範にわたる。）

② DoS 攻撃

・ 大量のアクセスが集中することで、サービスが停止させられる。従来、DoS 攻撃は利用者側で対処できたが、クラウド・サービスでは事業者側の対策に委ねなければならない。大手事業者ほど標的となりやすい。

③ マルチテナントの利用集中によるアプリケーション品質の低下

・ 複数の利用者がソフトウェアやデータベースを共有しているマルチテナントでは、特定の時間にサービス利用が集中すると、パフォーマンスが低下する。その結果として、利用者側の業務遂行に支障が生じる。

④ アプリケーションの脆弱性発見に伴うサービス停止

・ プログラムやアプリケーションの構成上の脆弱性が発見された場合、事業者側がサービスを一斉停止させることがあり、その間、利用者側は業務を継続できなくなる。

(3) 法的リスク、カントリーリスク

① 保管場所における法務リスク

・ データをさまざまな国に分散保持する場合、その国の法令に基づきデータ開示義務が生じたり、著作権の規制を受けたりすることがある。

② 設置場所のカントリーリスク

・ データセンタ設置場所(国)における自然災害や治安悪化、インフラ機能(電力供給等)の停止による影響を受ける。

上記のようにクラウド・サービスをとりまくリスクは様々であり、すべてのリスクを取り除くことは、困難と言わざるを得ない。自組織の業態、状況、事業規模、システム構築状況等に応じて優先的に対応するべきリスクを特定することが重要である。また、そのようなリスクに対して高いレベルでのリスクマネジメントを実現しているクラウド・サービス事業者を見極めていく必要がある。

6. セキュリティを考慮したクラウド・サービスの選定のポイント

クラウド・サービスを利用した場合、組織の事業遂行の根幹を成す情報資産のほとんどを外部組織であるクラウド事業者に依存することになるため、情報セキュリティに関するさまざまなリスクの洗い出し、評価、管理が難しくなる。すなわち、クラウド・サービス利用時の情報セキュリティマネジメントは、組織内の従業員はもとよりクラウド事業者の協力が最低条件となってくる。しかしながら、クラウド事業者は独立した組織であるため、情報セキュリティレベルはクラウド事業者によってコントロールされることになる。したがって、利用者が自社のセキュリティレベルを確立するためには、事業者に情報セキュリティレベルに関する情報を開示するように協力を求めていくことが重要である。

この観点から、クラウド事業者の選定に当たっては、先に紹介した経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を遵守しているかどうか、あるいは国際標準規格「ISO/IEC27002：2005」や日本工業規格「JIS Q 27002（情報セキュリティマネジメント実践のための規範）」に準拠しているかどうかを確認することが極めて有効な手段となる。

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（経済産業省）

クラウド利用者がクラウドサービスを利用する際に、情報セキュリティ確保のためクラウド利用者が自ら行うべきこと、およびクラウド事業者に対して求める必要のあること等についてまとめたもの。
本ガイドラインは、情報セキュリティマネジメントの国際的な規格（ISO/IEC27002:2005）をベースとし、クラウド利用の視点から各項目をまとめている。クラウド利用・活用の際の利用者・事業者双方のコミュニケーションツールとして活用できる。
（http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloud_security_guideline.pdf）

「JIS Q 27002(情報セキュリティマネジメントの実践のための規範)」
情報セキュリティマネジメントの共通に受容できる目標に関する一般的な手引き。組織における情報セキュリティマネジメントの導入、実施、維持および改善のための指針、および一般原則についての標準化を行い、生産および使用の合理化、品質の向上を図るために制定されたもの。

さらには、クラウド・サービスの規約の BCP（事業継続計画）関連規程を確認することも重要である。地震をはじめとした自然災害や大規模停電など有事の際に、クラウド事業者が何時、どのような手順で復旧を図るのかを把握することは、自社の情報セキュリティマネジメント、あるいは BCP（事業継続計画時期）を構築するに当たっての礎となる。

本稿がクラウド・サービスをとりまくリスクを理解し、また具体的に講じるべき対策を検討する際の一助になれば幸いである。

インターリスク総研 コンサルティング第二部 BCM 第二グループ
コンサルタント 小鍛冶 勝 （コカジ マサル）

（参考文献）

- 『クラウドサービス安全利用のすすめ』 独立行政法人情報処理推進機構セキュリティセンター
- 『クラウドサービス利用のための情報セキュリティマネジメントガイドライン』 経済産業省
- 『スマート・クラウド研究会報告書』 スマート・クラウド研究会
- 『国内クラウドサービス市場ユーザー動向調査結果』 IDC Japan
- 『高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する報告書』 経済産業省