クラウドコンピューティングの
社会インフラとしての特性と緊急時対応における課題
に関する調査
－　調査報告書　－

2012 年 9 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

［改訂履歴］

日付	改訂内容
2012 年 9 月 28 日	報告書初版発行
2012 年 10 月 9 日	東日本大震災におけるクラウドの利活用の実態と課題　事例の追加

調査実施者：

株式会社野村総合研究所

独立行政法人情報処理推進機構
技術本部セキュリティセンター
情報セキュリティ分析ラボラトリー

目次

調査の背景と目的 1

I. クラウドが社会インフラとして浸透している実態とその機能停止が社会経済に与える影響の定性的評価 3

1. クラウドの社会インフラとしての浸透の実態と課題（実態調査その1） 3

1.1. 個人間の通信・情報共有手段のサービス基盤としてのクラウド 4

1.2. 消費者向け電子商取引のシステム基盤としてのクラウド 19

1.3. 企業の生産販売、企業間情報連携等の情報インフラとしてのクラウド 36

1.4. 重要インフラ等の情報インフラとしてのクラウド 58

2. 東日本大震災におけるクラウドの利活用の実態と課題（実態調査その2） 73

2.1. 調査の概要 73

2.2. 調査の方法 73

2.3. 調査の結果 73

2.4. 東日本大震災に関するクラウドサービスの有効性の検証結果 114

3. 東日本大震災におけるデータセンターの緊急対応の実態と課題（実態調査その3） 116

3.1. 調査の概要 116

3.2. 調査の方法 116

3.3. 大規模災害時におけるデータセンターの対応と課題 117

4. クラウドの機能停止が社会に与える影響の定性的評価 139

4.1. 実態調査のまとめ 139

4.2. クラウド停止の影響 140

4.3. 最近発生したクラウドの大規模障害とそこから抽出されるセキュリティ課題 141

II. クラウドが備えるべきレジリエンシ及びディペンダビリティを実現するためにクラウド事業者ならびに社会システムが満たすべき要件の調査 143

1. 問題認識 143

2. 現状の取り組みと課題 144

2.1. 対応の前提となる想定リスクの考え方を見直す必要性 144

2.2. データ・システムのバックアップの確保に関する現状 145

2.3. BCP（事業継続計画）による準備の現状 147

2.4. 平常時からのファシリティ面の対策 147
2.5. 平常時におけるライフラインの冗長性確保 148
2.6. 緊急･災害時における代替ライフラインの確保 149
2.7. 緊急･災害時における代替ライフライン確保のための二次的サプライの要件 .. 149
2.8. データセンターの運転ならびに保安のための要員に関する要件 149
2.9. 緊急・災害時におけるセキュリティ対策、ならびに意図を持って行われるサイバー攻撃に対する防衛または回避 150
2.10. 中小事業者、ベンチャー等の提供するクラウドサービスのリスクへの対応 151
3. クラウド事業者ならびに社会システムが満たすべき要件 152
3.1. 想定外のリスクならびに動的なリスクへの対応 152
3.2. トリアージの枠組みにおける考え方の例 157
3.3. 個別の取り組みで満たすべき要件 162

III. システムやベンダーの枠を越えたデータセンター間連携やクラウド間マイグレーションを可能にするために必要な諸要素の調査 164

1. 問題認識 164
1.1. 欧米の動向 164
1.2. 日本の動向 165
2. 現状の取り組みと課題 167
2.1. 事業者の認識 167
2.2. 先行的な取り組み事例 167
3. クラウド間連携等の実現に向けた諸要素 169
3.1. クラウド間連携がスムーズに実現するための技術的要件 169
3.2. クラウド間連携における契約や取り決め等の要件 175

IV. 今後官民が取り組むべき課題の提起 180

1. クラウド事業者およびその他の事業者、社会システムが満たすべき要件の全体像 180
2. 官民が取り組むべき課題 181
2.1. 基本的な考え方 181
2.2. 具体的な施策 183

おわりに 185

調査の背景と目的

クラウドコンピューティング [1]の社会への普及が進んでいる。従来はオンプレミス [2]で運用されてきた企業や行政機関の業務システム、水道などのライフラインの管理システム、電子カルテなどの医療に関するシステムなど様々な重要インフラに属するシステムにおいてもクラウドコンピューティングが用いられるようになってきている。また、様々な消費者向けクラウドサービス [3]の出現により、一般国民が生活で利用する電子商取引やエンターテインメント、個人のコミュニケーションやデータの格納などでの利用も活発に行われている。それらが震災等の非常時対応に役立つ要素があることを踏まえると、クラウドコンピューティングはもはや「社会インフラ」になりつつあると言え、その利用はさらに拡大すると予想される。

しかし、地震、津波、風水害などの様々な自然災害による、クラウド [4]を担うデータセンターの被災、通信回線の不通、電源喪失または電源不足等の原因や、近年著しいサイバー攻撃によってクラウドコンピューティングが停止した場合に、社会経済や国民生活に及ぼす影響の規模と範囲ならびに被害の深刻さが、従来考えられていたよりも広がっていることが想定される。

このように、クラウドコンピューティングがさらに普及し、社会インフラとしての役割の重さが増すことに伴って、これらの災害や情報セキュリティリスクに対する耐性が強く求められることになる。特に、ITシステム等が外部環境の変化による障害等に遭っても所期の機能・状態に一定程度回復する能力「高回復力性＝レジリエンシ（resiliency）[5]」や構成要素の一部の不具合による影響を排除して、外部に対して所期の機能やサービスを提供し続ける能力「機能保障能力＝ディペンダビリティ（dependability）[6]」の向上が必要であると考えられる。

本調査においては、上記の視点からクラウドコンピューティングが社会インフラとして浸透していく中で、その役割を果すために充足すべき課題を明らかにすることを目的として、以下の内容について調査検討を行った。

- クラウドコンピューティングの社会インフラとしての普及実態の把握
- 社会インフラとして求められるの高回復力性、機能保障能力の視点からの事業継続ならびに情報セキュリティ・緊急時対応に関する課題の抽出
- 緊急時対応における課題を解決し、社会インフラとしてのサービスを継続していくた

---

1 大規模データセンターにおいて仮想化等の技術を用いてコンピュータの機能を用意し、それをインターネット経由で自由に柔軟に利用する仕組みの総称。

2 情報システムにおいて自社で用意した設備でソフトウェアなどを導入・利用する自社運用のこと。

3 クラウドコンピューティングに基づいてサービスの形で提供される IT の機能。

4 クラウドコンピューティングおよび／またはクラウドサービス。

5 広義には、「インシデントに影響されることに抵抗する組織の能力」（事業継続マネジメントシステム BS25999）とされる。

6 「実行された仕事（service）がどの程度正しく行われているかを明らかにするための品質（quality）を示すもの」（J.C. Laprie, 1985）という定義を参考とした。

め、システムやクラウド事業者[7]の枠を越えた連携やマイグレーションを可能とするために必要な諸要素の把握

- これら社会インフラとして求められる特性を実現していくために官民が取り組むべき課題の抽出

7 クラウドコンピューティングまたはクラウドサービスを提供する事業者。

I. クラウドが社会インフラとして浸透している実態とその機能停止が社会経済に与える影響の定性的評価

1. クラウドの社会インフラとしての浸透の実態と課題（実態調査その１）

本節では、クラウドが社会インフラとして広範に浸透している実態を把握するとともに、大規模災害やサイバー攻撃等によって機能停止に陥った場合の影響の度合いを明らかにするため、文献調査、インタビュー、ならびにアンケート調査を行った。

対象分野は以下の 4 つの領域における情報システム基盤である。

・ メールやソーシャルネットワーキングサービス（SNS）等の個人間の通信・情報共有手段

これらのサービスは、先の東日本大震災において固定電話や携帯電話などに並んで、被災状況や救援依頼、安否確認等に大きな力を発揮した。そのため、今後も個人間の有力な通信・情報共有手段として成長していくものと考えられる。また、スマートフォン等の端末機器の発達と相まって、「つぶやき」や写真投稿による個人の情報発信や、「チェックイン」による位置情報等の情報収集を容易に行えるようになっており、緊急時に現場末端の生の情報を収集するプラットフォームとしても重要となってきている。

・ 消費者向けの電子商取引（BtoC EC[8]）

ネット通販やネットスーパーに代表される BtoC EC は、過疎化が進む地方等において日常生活を支える商店が失われた状況においても、住民の生活を支える大きな役割を担っている。今回の震災の被災地においても仮設店舗や移動販売等と並んで住民のライフラインを支えたとみられている。

・ 企業の生産販売や企業間情報連携（BtoB[9]）

企業の生産活動はIT[10]に大きく依存している。また生産販売活動における企業間の分担・連携、いわゆるサプライチェーンは高度に複雑に発達している。先の震災において、東北地方に所在する製造業が被災し生産が停止したことで、ここから出荷される部品の供給が停止したことから、国内の他地域のみならず海外においてもサプライチェーンに大きな影響を及ぼした。このことから、企業の受発注や生産販売管理等のサプライチェーンマネジメントに用いられるコンピュータシステムが停止した場合には、経済社会に対して与える影響も大きいものと考えられる。

・ 重要インフラ等の社会基盤

内閣官房情報セキュリティセンター（NISC[11]）では、情報通信や金融等の 10 分野

8 Business to Consumer Electronic Commerce
9 Business to Business
10 Information Technology 情報技術
11 National Inforamtion Security Center

を「重要インフラ」として指定している。これらの重要インフラが、情報システムの停止によりサービスを停止するとすれば、社会に与える影響は非常に大きいと考えられる。

次項からは、上記の 4 分野それぞれについて調査結果を述べる。

1.1. 個人間の通信・情報共有手段のサービス基盤としてのクラウド

1.1.1. 調査の概要

本項では、個人間の通信・情報共有手段の代表的サービスであるソーシャルネットワーキングサービス（以下、SNS）やメールサービスにおける、同サービス運営上でのクラウドへの依存度について、図表 1 に示した SNS・メールサービス事業者への聞き取りや文献などにより把握した。

SNS およびメールサービスを運営する企業は、データセンターを自社で所有しているケースが多く、内部のシステムではクラウドコンピューティングを採用していない例もあると考えられるが、サービスのエンドユーザが情報等を外部ネットワークに保存できる、という意味ではクラウドサービスの定義に該当すると考え、調査を行った。

図表 1 調査対象事例

事例名称	概要
Google	• Web 検索サービスを母体としたポータルサイト
mixi	• ソーシャルネットワーキングサービス（日記、メッセージなど提供）
Windows Live	• 電子メールを含む Web サービスとクライアントソフトウェア（アプリケーション）
Yahoo! Japan	• Web ディレクトリサービスを母体としたポータルサイト
@nifty	• 電子メールやブログを含む Web サービスを母体としたポータルサイト
地域 SNS	• 地域コミュニティに根付いたソーシャルネットワーキングサービス

1.1.2. 対象事例

（1） Google （米 Google Inc./グーグル株式会社）

① サービスの概要

Google は 1998 年に米国で創業された、ウェブ検索サービスを母体にしたポータルサイトである。近年では、メールサービス Gmail を初め、多様な個人向けの無料サービスを提供しているほか、スマートフォン用 OS の Android やウェブブラウザの Chrome などのソフトウェアプロダクトも発表し、無償配布している。

② サービスの普及度

Googleは全体のユーザ数を体系的には明らかにしていないが、いくつかのサービスにおいて、利用者数が断片的に発表されている。Gmailの利用者数は 2012 年 4 月の同社からの発表 [12]によれば全世界で 3.5 億アカウント、Google+では、2012 年 3 月の発表 [13]によれば月間アクティブユーザ数は 1 億人超、1 日のアクティブユーザ数は 5,000 万人である。

なお、これらのユーザ数には個人だけではなく法人ユーザも含まれている。

③ Google のクラウド利用の状況

Google のサービスにはポータルサイトを中心とした個人向けサービスの他、業務向けクラウドサービスである Google Apps for Business / Education が存在するが、本項では個人向けサービスについて述べる。

日本国内で利用できる個人向けのコミュニケーションサービスの主なものは以下の通りである。これらはいずれも Google の構築したクラウド上での SaaS として提供される。

- Gmail：電子メールサービス
- Google ドキュメント：文書、スプレッドシート、プレゼンテーションの作成アプリケーションの SaaS
- Google カレンダー：予定表、連絡先、To-Do 管理等の SaaS
- Google グループ：グループウェアの SaaS
- Google+：ソーシャルネットワーキングサービス
- Google ドライブ：オンラインストレージサービス

内部システムから見ても、Google のサービスの大半は数ペタバイトにも及ぶ大

---

12 Googel Inc. “2012 Update from the CEO” http://investor.google.com/corporate/2012/ceo-letter.html

13 発表の原文は入手できないが、インプレス社「InternetWatch」（http://internet.watch.impress.co.jp/docs/news/20120307_517083.html）等で報道されている

規模データを、世界中に設置している数十万台のサーバに格納した巨大分散データストアである Bigtable を運用基盤として提供されている。

④ 障害事例とその影響

2012 年 4 月 18 日午前 1 時頃（日本時間）、Gmail にアクセスできないという障害が発生した。全ユーザの 10%弱に影響があったとされる。メールの消失等は発表されていないが、障害に巻き込まれたアカウントではメールの配送が遅延する可能性があるとしている。この障害は、発生して約 1 時間後にすべての影響アカウントで復旧している。先に述べた Gmail のユーザ数 3.5 億人から推定すると、2012 年 4 月の障害によって、日本の首都圏の人口に匹敵する 3,500 万人程度が、約 1 時間電子メールの利用ができなかったことになる。

Gmail では 2011 年 2 月にもストレージソフトウェアのアップデートの際にソフトのバグによる障害を起こしている。このときにはユーザの 0.02%に影響があり、一部のユーザのメールが消失する問題が発生している。このときにはバックアップデータなどからのメールの復旧を行っている。

このようにクラウドサービスの利用が普及したため、障害の影響が大規模に及ぶようになったことが、実例でも改めて明らかになったと言える。

⑤ 東日本大震災時の対応・利用状況

東日本大震災においては、個人の安否確認や被災地支援のために「Crisis Response」を提供した。同サービスは 2005 年にハリケーン・カトリーナが米国を襲った際に被災者とその周辺が必要な情報を常に取得できるように提供を開始し、専用のサービスチームを配置する事で 24 時間体制での対応を可能にしている。

震災発生から 2 時間後には同サービスの日本語版を公開し、被災者の検索および情報取得の機能をもつ「パーソンファインダー」の利用を可能にした。「パーソンファインダー」は安否情報をユーザが簡単に登録・閲覧できるもので、登録件数は開始直後には約 3,000 件だったが、翌月には 60 万件超を記録した。グーグル社は各自治体やメディアとの連携を早め、情報公開用のファイルフォーマットも公開フォーマットである PFIF[14]を使用するなど、データ統合を容易にしている。震災発生の翌月である 2011 年 4 月には、「パーソンファインダー」のペット版である「アニマルファインダー」も公開している。

また、動画配信サービスである「Youtube」において、発災直後から TV ニュース番組のライブストリーミングを提供した。それ以外にも、「Google マップ」による被災地の衛星および航空写真の提供、交通遅延情報およびそのタイムテーブルの提供、東北地方のビジネスを支援するサイト・チャンネルの提供なども行い、積極的

14 PeopleFinder Interchange Format 被災者情報共有のための XML ベースのデータフォーマット

に震災後の情報整理や復興支援に寄与している。

このように日常だけではなく、大規模災害時においても個人のコミュニケーション手段を確保するとともに、状況に応じた柔軟なサービスの提供が可能であることが確認された。

(2) mixi(株式会社ミクシィ)

① サービスの概要

mixi は日本における SNS(ソーシャルネットワーキングサービス)で最大規模を誇っている。主なサービス内容は、以下のようなものがある。

- ユーザ個人の投稿を起点とし、コメントや「いいね!」ボタンの反応等でコミュニケーションを図るもの:日記、mixi ボイス、フォト、動画、レビュー、mixi チェックなど
- ユーザの 1 対 1 のコミュニケーション:メッセージ
- ユーザが開設したグループでのコミュニケーション:コミュニティ
- ソーシャルアプリケーションやソーシャルゲームを仲介としたコミュニケーション:mixi アプリ

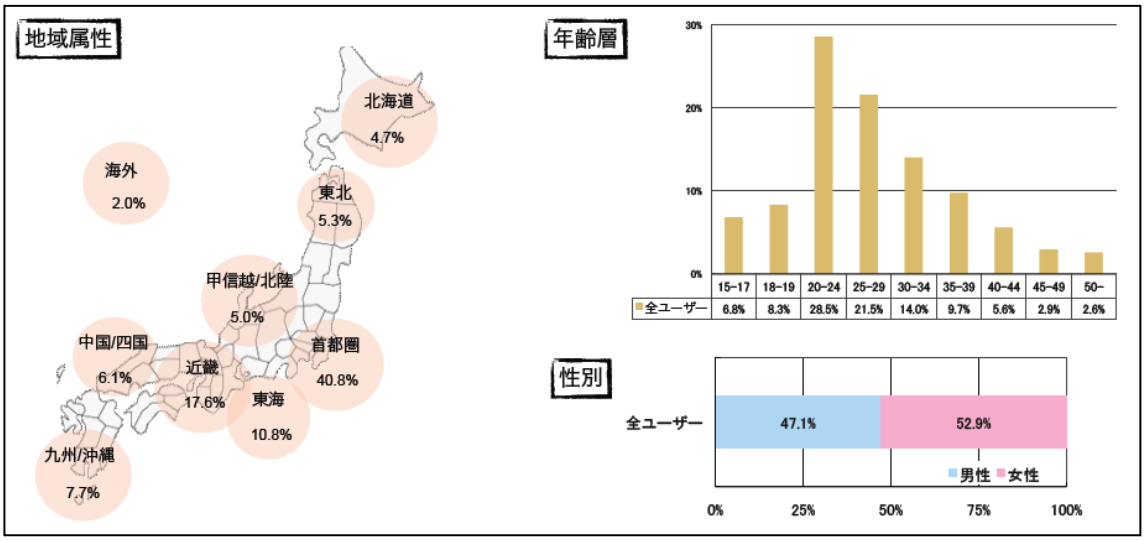
② サービスの普及度

2012 年 3 月時点での登録ユーザ数は 2,711 万人、うち月に 1 回でもログインしたユーザが 1,512 万人である。サービス開始以来、ユーザの投稿数は 7 億回を超える。

ユーザ属性を見ると、年齢では 20 代と 30 代が中心になっており、性別で見ると、男性が 47%、女性が 53%となっている。地域別に見ると、首都圏が全ユーザ中 40%と圧倒的に多く、近畿の 17%がそれに続く。

利用実績は、2012 年 3 月の総ページビュー(PV)が 200 億 PV 程度であった。

図表 2 mixi の会員属性



出所）株式会社ミクシィ 2011 年度　通期決算説明資料
http://v4.eir-parts.net/DocumentTemp/20120731_111436874_es4zxjmccblpfgylylkx2a45_0.pdf
（2012 年 6 月現在）

③ クラウドの利用状況

mixi のサービスのうち、mixi アプリと呼ばれるソーシャルアプリケーションは、外部のクラウドサービス（Microsoft、ニフティ、Amazon、Google など）と連携して提供されている。mixi アプリは、サードパーティでも開発・提供が可能であり、サードパーティは mixi が持つ顧客基盤や課金プラットフォームなどを利用して、mixi 会員を対象としたサービス提供とビジネス展開が可能となっている。

mixi アプリの公開後のユーザ数の増加が急激であること、ユーザ数の伸びが鈍化してからもリクエストが多いことがアクセスの特徴として上げられており、mixi アプリ提供者にはサービスを停止させないためにサーバ等の能力の整備が求められている。なかでもクリスマス等のイベント時におけるキャンペーンと連動したソーシャルアプリにおいては、短期間に大容量のアクセスが発生し、時限的に終了するといった特徴があり、クラウドが多く利用されている。これは、クラウドサービスの特徴であるサービス立ち上げの速さやスケーラビリティ確保の容易さなどを活かした利用方法と言える。

たとえば毎年クリスマスシーズンに提供される「mixi クリスマス」は、アプリケーションに表示されたクリスマスベルを鳴らすことで、キャンペーンの当選確率が上がるなどの特徴を持ったアプリである。2011 年は 11 月 30 日から 12 月 25 日まで公開された。12 月 20 日の時点で 250 万人の登録があった。期間中は 1 日平均 110 万人以上がアクセスし、約 1.8 億回以上もベルが鳴らされるなど、膨大なアクセスがあったことがうかがえる。

この mixi アプリのサービス基盤はマイクロソフトが提供する Windows Azure Platform を用いている。ユーザの急激な伸びに対する、インフラの迅速な拡張などの対応が、円滑に行われたとされている。

なお、この他のサービスの内部システムについては、クラウドコンピューティングの技術を用いていないとのことであった。

④ 障害事例とその影響

mixiでは 2010 年 8 月 10 日に断続的にアクセスがしづらくなる障害が発生した。同社の発表[15]によると、データキャッシュシステムの不具合により、8 月 10 日と翌 11 日の 2 度にわたって障害が発生し、サービス閲覧を中止して復旧作業を行った。最終的に問題が解消したのは 31 時間後であった。

1 日以上のサービス停止によって、単純計算で月間利用の 3～4%程度に影響が出たと考えられる。前述した月間 200 億 PV から推定すると、6～8 億 PV に相当するトラフィックが失われたことになる。このことは、ユーザ側から見ると、情報入手あるいはコミュニケーションの機会が、6～8 億回分失われたことになるとも考えられる。

⑤ 東日本大震災時の対応・利用状況

東日本大震災では、全体ユーザの 5.4%を占める東北のユーザとその周辺を中心に、「mixi」の各種機能を用いた被災地・被災者についての情報交換が活発に行われたことが報告されている[16]。

mixi の SNS としての本来の機能が、ユーザの創意工夫によって安否確認に活用されている。その代表的な例は以下の通りである。

・ mixi 上の友人「マイミクシィ」のログイン時間表示の確認
・ 日記や一言メッセージ「mixi ボイス」投稿の確認
・ 位置情報公開サービス「mixi チェックイン」の確認

このうち 1 番目は、マイミクシィのリスト表示において、それぞれのマイミクシィが最後にログインした時刻を「1 時間以内」「1 日以内」のように表示できるため、これを安否確認に用いたものである。すなわち、最近にログインが行われている表示があれば、生存が確認できることになる。運営側でもこのような利用に応えるため、2011 年 3 月 16 日には、マイミクシィ登録しているユーザのログイン履歴が一覧で閲覧できるウェブページを設置し、各ユーザがより簡単に被災者の状況を把握できるようにした。また、2 番目はユーザが書き込める日記やより短いメッセージであ

15 株式会社ミクシィ報道発表資料（2010 年 8 月 12 日）
http://mixi.co.jp/wp-content/uploads/2010/08/20100812.pdf （2012 年 6 月現在）

16 総務省「大規模災害等緊急事態における通信確保の在り方に関する検討会 インターネット利用ワーキンググループ」 第 3 回 資料 3-5 株式会社ミクシィ説明資料
http://www.soumu.go.jp/main_content/000120217.pdf （2012 年 6 月現在）

るボイスの書き込みを見て、そのユーザの安否を確認するものである。これらの書き込みはスマートフォンや通常の携帯電話からも容易に行えるため、個人の安否確認には有用であった。さらに 3 番目のサービスは、携帯電話ならびにスマートフォンから位置情報を付して mixi に簡単なメッセージを投稿するもので、通常はレストランなどの街情報に関する情報などが書き込まれる。これを現在位置登録に使う例が見られ、mixi 上の友人に自らの安全と所在を明らかにするために用いられた。

また、震災関連情報を交換できるコミュニティを地域別（市町村、自治体など）や目的別（救援物資、炊き出しなど）に分けて作成し、情報の整理を行った。そのうちの大きなコミュニティでは約 35 万ユーザの参加が確認されている。

このような利用によってmixiへのアクセスが増加した。mixiボイスでは、平常時の利用に比べ震災直後は投稿数が 8 倍に増加し、その後数日にわたり平常時の 2 倍程度の投稿が行われた。写真などと合わせて投稿できる日記は、被災地である東北エリアからの投稿数が平常時に比べ 44%増加した。

これに対応して運営者側もサーバを平常時よりも数台多く設置し、急激なアクセス増加に備えた。他の設備面も確認し、電力供給などインフラ面での問題がない限り非常時におけるサービスの継続も平常時と変わらず行えるように対応を行った。

（3） Windows Live （Microsoft Corp./日本マイクロソフト株式会社）

① サービスの概要

Windows Live はマイクロソフトがユーザに無償で提供する Web サービスとアプリケーションを総称したサービスブランドである。その主なサービス内容は以下の通りである。

Web サービス

- Hotmail：Web メールサービス
- SkyDrive：オンラインストレージサービス
- カレンダー：メールクライアント同期が可能な予定表サービス
- フォト：オンラインフォトアルバムサービス

クライアントソフトウェア

- メール：電子メールクライアント
- Writer：ブログ編集
- ムービーメーカー：動画編集、共有
- フォトギャラリー：写真、動画の管理、編集、共有
- Messenger：テキスト、音声、ビデオチャット

② サービスの普及度

Hotmail は公称 3 億 6 千万人のユーザを有しており、Gmail 以上の規模を持つ。

国内ユーザのプロファイルは、日本マイクロソフトが発行する広告主向け媒体資料によると、男性 48%、女性 52%であり、性・年代別には女性 20～34 歳（約 25%）、男性 20～34 歳、同 50 歳以上、同 35～49 歳（いずれも 15%台）の順に多い。

③ クラウドの利用状況

電子メール、オンラインストレージ、カレンダー、フォトアルバムから成る Web サービスは、クラウドサービスによって提供されている。クライアントソフトウェアと呼ばれるアプリケーションは、それら Web サービスを利用するためにマイクロソフトから提供されている。ユーザは自身の情報端末からこれらアプリケーションにアクセスすることでサービスを利用できる。

このほかに、マイクロソフトのデスクトップアプリケーションをクラウドで提供する有料サービス「Office365」があり、個人や中小企業のユーザを獲得している。

④ 障害事例とその影響

2011 年 9 月 8 日、HotmailとSkyDriveを含むWindows LiveサービスとOffice 365 サービスに 2 時間半にわたってアクセス障害が発生した。マイクロソフトでは代替サービスを立ち上げたが、DNS[17]の書き換えを伴ったため、ネットワーク全体への波及に時間を要し、全ユーザがアクセス可能になるまでにはさらに相当の時間を要した。このトラブルの原因は、米国内における停電の影響と言われている。

Hotmail では 2010 年 10 月 31 日（日）午前 7 時～11 月 4 日（木）午前 11 時頃にも日本国内ユーザ（当時のアクティブアカウント約 510 万）のうち、最大 9.4 万アカウントにアクセス障害と一部のユーザのメール消失が発生している。この原因は日本国内におけるサーバのハードウェア障害であったと言われている。

このように、クラウドを利用する際には、リスクが複数の場所に分散することにも留意する必要がある。

（4） Yahoo! Japan （ヤフー株式会社）

① サービスの概要

Yahoo! Japan は、ウェブディレクトリサービスを起源に持つポータルサイトであ

[17] Domain Name Service

る。メールやオークション、ショッピングなど多様なサービスを提供している。本節の対象となる個人のコミュニケーションに関わるサービスは以下の通りである。

- Yahoo! Japan メール：Web メールサービス
- カレンダー：予定表の SaaS
- アドレス帳：住所録の SaaS
- 掲示板：ユーザが自由にテーマを設定し、ディスカッションを行う BBS（Bulletin Board System）サービス
- グループ：グループウェアの SaaS
- ブログ：日記などを記入、公開できるサービス
- メッセンジャー：チャットなどを提供する IM（Instant Messenger）サービス
- Yahoo!ボックス：オンラインストレージサービス
- Yahoo! Japan オークション：個人でも出品できるオークションサービス

② サービスの普及度

Yahoo! Japanでは無料会員と有料のプレミアム会員が存在している。無料・有料会員を合わせた月間のアクティブユーザ数は 2012 年 1～3 月の平均で 2,640 万人、プレミアム会員は2012年3月末で780万人となっている[18]。全国民の20%に当たるユーザがアクティブにアクセスしている計算になる。

また、Yahoo! Japanメールのアクティブユーザ数は2010年11月末現在1,750万人[19]、Yahoo!ボックスのユーザ数は 2012 年 1 月現在 100 万人[20]である。

③ クラウドの利用状況

Yahoo! Japan の個人のコミュニケーション手段として提供されているサービスのうち、クラウドを利用しているのは Yahoo! Japan メールと Yahoo! ボックスが代表的なものである。

他のサービスについても、SaaS として提供されており、エンドユーザから見た姿はクラウドサービスと見ることができる。

---

18 ヤフー株式会社 2011 年度第 4 四半期および通期決算説明会プレゼンテーション資料 http://i.yimg.jp/i/docs/ir/archives/present/2012/jp0424present-all.pdf（2012 年 6 月現在）

19 総務省「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」迷惑メールの対応の在り方に関する検討 WG（第 4 回会合）（2010 年 12 月 20 日） 資料 1「迷惑メール報告機能」について（ヤフー株式会社） http://www.soumu.go.jp/menu_sosiki/kenkyu/riyousya_ict/39449.html（2012 年 6 月現在）

20 Yahoo! Japan 広報からのお知らせ（2012 年 1 月 20 日） http://blogs.yahoo.co.jp/yj_pr_blog/22069576.html（2012 年 6 月現在）

④ 障害事例とその影響

Yahoo! Japan では 2010 年 10 月 13 日 23 時 30 分ごろから同サイトのトップページに接続できない障害が発生した。他のサービスのページは機能していたが、トップページが接続不可だったため、各サービスのページに接続しにくい状態になっていた。約 2 時間後に復旧した。後日、原因はロードバランサーのハードウェア障害であることが明らかとなった。

Yahoo! Japan では同様のシステム障害が各サービスにて小規模に発生して接続しにくくなることはあったが、この場合は全てのサービスの入り口となるトップページの接続障害であり、全サービスへの接続に影響を及ぼした。本事例は、ウェブサービスの起点となる部分の影響力がいかに大きいかを示した事例と言える。

⑤ 東日本大震災時の対応・利用状況

ヤフー株式会社からの報告[21]によれば、Yahoo! Japanでは大規模災害等の非常時における対応について準備を進めていた。震度 3 以上の地震が発生するとヤフー内の震災関連サービスの担当者全員にメールで通知が届き、震度 6 以上の場合は担当者が時間に関わらず出社して対応にあたる。2005 年からは、それまで東京オフィスのみで行っていたウェブサイトの更新・編集機能を大阪オフィスにも設置して二重化を図っていた。

このような準備もあり、東日本大震災が発生した際も迅速な対応が可能であった。震災直後の 2011 年 3 月 14 日には、サイト開設以来最高となる 23 億 6500 万 PV のアクセス数を達成している。被災地からのアクセスは通常の 40%程度だったものの、インターネットによる災害情報の受発信に大きく役立ったと言える。

コンテンツにおいても災害対応を行った。災害関連情報をまとめた特設ページを開設し、災害関連の情報を一元的に閲覧できるようにしたほか、「Yahoo! ボランティア」ページでは震災直後から被災地・被災者向けの募金受付を開始し、「Yahoo! 天気情報」ページでは NHK のニュース映像のライブ配信を行った。こうした複数のページにわたる同時対応にあたっては、各ページの担当者間でのYahoo!メッセンジャーによる連絡が活用された。

震災の経験を踏まえ、2011 年 7 月に「Yahoo!メッセンジャー」上で各種災害情報を受け取れるサービスである「防災速報」を開始するなど、災害時の情報提供機能を強化している。

---

21 総務省「大規模災害等緊急事態における通信確保の在り方に関する検討会 インターネット利用ワーキンググループ」 第 3 回 資料 3-2 古閑構成員（ヤフー株式会社）説明資料
http://www.soumu.go.jp/main_content/000120214.pdf （2012 年 6 月現在）

(5) @nifty （ニフティ株式会社）

① サービスの概要

@niftyはパソコン通信のnifty-serveを起源に持つ、接続事業者系のポータルサイトサービスである。接続会員向けに始められたメールや情報サービスから発展して、現在では接続サービスを利用しなくても有料または無料でサービスを利用することができる。本節の対象となる個人のコミュニケーションに関わる主要なサービスは以下の通りである。

- mail@nifty：メールサービス
- @nifty ココログ：日記などを記入、公開できるブログサービス
- @nifty マイキャビ：オンラインストレージサービス
- @nifty バックアップ：PC のクラウドへのバックアップサービス
- @nifty ホームページサービス：Web ページのホスティング

② サービスの普及度

ISP接続サービス会員を含めた会員数は2012年3月現在で1,170万人である。このうちISP接続会員（174 万人）を除いた、各種サービスのみを利用している会員は996万人である[22]。

③ クラウドの利用状況

Web サービスの一環として、個人向けメールと法人向けのビジネスメールを提供している。ニフティ自身の認識はWebサービスであるが、Gmailと同様のクラウドベースのメールサービスである。以前よりサーバは仮想化技術を用いている。

このほかにニフティクラウドとしてIaaSサービスを行っている。

④ 障害事例とその影響

2012年6月7日、個人向けメールおよび法人向けのビジネスメールサービス、ブログサービス「ココログ」、ニフティクラウドにアクセスおよび利用がしにくい状況が発生した。影響を受けた全てのサービスが障害から復旧するまでには 12 時間以上を要した。この原因は同社の発表 [23]によるとデータセンターの電源装置の故障とされている。

この際、ブログサービス「ココログ」にてハードウェアの数を減らした縮退運用を一時的に行わざるを得なかった結果、ユーザによる日記投稿などに遅延が生じる2次障害が24時間以上に渡って発生した。

---

22 ニフティ株式会社「2011 年度通期決算説明会プレゼンテーション資料」
http://www.nifty.co.jp/ir/pdf/20120426_01.pdf（2012 年 6 月現在）

23 ニフティ株式会社「6 月 7 日に発生した大規模障害の復旧について」
http://www.nifty.co.jp/release/2012/pdf/nifty20120608.pdf （2012 年 6 月現在）

⑤ 東日本大震災時の対応・利用状況

ニフティでは過去に阪神淡路大震災でも支援活動を行った経験を活かし、ボランティアサイトの認証システムを開発・提供したほか、被災地で見つかった写真をクリーニングしてクラウド上で公開し、所有者を探すシステムの「思いでサルベージオンライン」など、複数のサービスの提供を行っている。また、自社サーバを所有している大企業に対して、計画停電や地震の再発に備え、システムの DNS を一時的にニフティのシステムに切り替えてデータの安全性、業務の継続性を担保する「メールの保険サービス」も、発災後数ヶ月に渡って提供を行った。詳細は、「2. 東日本大震災におけるクラウドの利活用の実態と課題(実態調査その 2)」で述べる。

(6) 地域 SNS

① サービスの概要

地域 SNS は、ICT を活用し地域社会の「人のつながり」を作り強化することで地域社会の活性化を目指す取り組みの一環として、2004 年の末に熊本県八代市で始まり、全国で急速に拡大している。地域 SNS は地元で開催されるイベントの掲載をはじめ、地元住民による日記や掲示板への投稿など、地元住民とそこへ訪れる観光客のコミュニケーションの場になっており、平時の利用以外にも、近年は災害発生時など非常時における活用に対する期待度が高くなっている。2008 年に発生した岩手・宮城内陸地震の際には、盛岡市の地域 SNS「モリオネット」で行われていたユーザ間の自発的な情報交換が、住民間での情報共有に役立った。

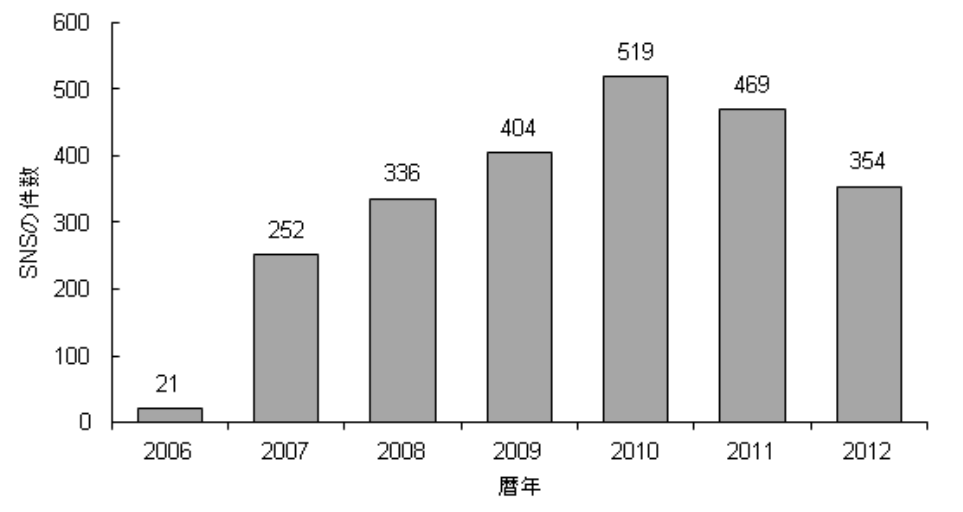
② サービスの普及度

国際大学 GLOCOM の調査では地域 SNS の事例は 2006 年 2 月には 21 事例だったのに対し、2010 年 2 月の 519 事例まで拡大したが、これををピークに減少を続けている。

代表的な地域 SNS プラットフォームの一つ、兵庫県のインフォミームが開発・運用する「OpenSNP」は、2011 年 2 月時点で以下のような規模となっている。これは、OpenSNP を利用して構築されている地域 SNS サービスの合計値である。

- 地域SNS登録者数:約 6,000 名
- アクセス数:101,400 件/月
- ページビュー:2,289,000PV/月
- データ転送量:60.54GB/月
- コミュニティ書き込み数:1,000 件/月
- ブログ書き込み数:15,800 件/月
- メッセージ数:14,000 件/月

図表 3 地域 SNS の運営数の推移



出所）地域 SNS 研究会 Web ページ
http://www.local-socio.net/2012/03/snssns354.html（2012 年 7 月現在）

③ クラウドの利用

地域 SNS は So-net 提供の ASP サービスを使った運用で 2006 年以来増加傾向にあったが、2010 年 6 月の So-net のサービス終了に伴い、閉鎖する SNS や、運営者が所有するサーバでの運用に移行する SNS が増えていた。このことが上述の減少傾向をもたらしたと考えられる。

しかし、東日本大震災発生時に、仙台市の河北新報社において自社の Web サイトが被災し情報発信ができなくなった際、クラウドサービス上で運営していた東北地域 SNS「ふらっと」に携帯電話回線で接続し、「ふらっと」を活用して情報発信を継続した事例が注目され、それをきっかけに地域 SNS が見直されている。

「ふらっと」などの事例を受け、「OpenSNP」など SNS プラットフォームを提供するクラウドサービスへの移行による、非常時に備えた対策を講じる地域 SNS が増加している。三重県松阪市の地域 SNS「松阪ベルネット」では、2011 年 6 月にそれまで設置していた自己保有サーバ上での運用から ASP 型に切り替えている。

1.1.3. クラウドの浸透実態と課題

本項で見てきた、SNS やメールサービス等の個人間の通信・情報共有手段におけるクラウドの利用状況、および障害事例とその影響等について、図表 4 にまとめた。個人向けに提供されているサービスにおけるクラウドの利用は、量的な拡大のみならず、提供されるサービスの種類も拡大しており、利用の範囲と態様が多

様化していることがわかる。

まず、量的な側面の拡大について見る。今回取り上げたサービスにおけるユーザ数はグローバルなサービスでは億人単位、国内中心のサービスであっても千万人単位に上っている。このことから、クラウド停止の影響は従来考えられていたよりも広範囲にわたることが予測される。実際に起こった障害事例においても数万人（homail の国内サービスの例）から数千万人（Gmail の例）と、多くのユーザに影響を与えている。

次に、適用サービスの多様化について見る。初期のクラウドサービスはメールサービスから始められていることが多かったと考えられる。その後、Google カレンダー、Google グループ等の個人・グループ向けの SaaS へと発展し、Yahoo!ボックス等のオンラインストレージやオンラインバックアップが提供されるに至っている。近年では、オンラインストレージサービスが発展して Instagram や YouTube 等の画像や動画を共有するサービスなども出てきている。

このことは、クラウドの障害の影響を受けるデータの種類が増えたことを意味する。以前であれば、影響を受けるのはメールであり、多くは着信時に目を通してしまえば用が済んでしまうような情報である。また必要があれば再送してもらうことも可能であった。ところが、オンラインストレージや共有サービス上に画像、動画、書類など多様なデータが置かれるようになれば、データが消失してしまうと再生不可能な情報も少なくないと考えられる。また、バックアップとしてクラウドを使った場合には、障害によってバックアップの機能を果たさないケースも考えられる。

一方、多くのサービスでメールアドレスを起点とするログイン認証を行っている。このことは、メールアドレスによるログインが障害を起こしてしまうと、あらゆるサービスにアクセスできなくなる可能性があることを示している。このように、一つのクラウドサービスの障害が、他のクラウドサービスの障害に連鎖していく可能性は、従来考えられていなかったリスクである。

以上のように、クラウドサービス利用の量的拡大と多様化によって、影響ユーザ数の増大、影響を受けるサービスやデータの拡大、さらにはクラウド障害の連鎖の恐れが高まっており、クラウドのサービス継続に対する要求がより高まってきているものと考えられる。

図表 4 調査対象事例のまとめ

サービス名	Google	mixi	Windows Live	Yahoo! Japan	@nifty	地域 SNS
主要な サービス内容	メール ドキュメント作成 SaaS カレンダーSaaS 住所録 SaaS グループウェア SaaS SNS オンラインストレージ	SNS （日記、メッセージ、画像・動画共有、コミュニティ等）	メール カレンダーSaaS オンラインストレージ オンラインフォトアルバム チャット	メール カレンダーSaaS 住所録 SaaS BBS グループウェア SaaS ブログ チャット オンラインストレージ	メール ブログ オンラインストレージ オンラインバックアップ ホームページ作成	SNS （日記、メッセージ、コミュニティ等）
サービスの普及度	Gmail：3.5 億アカウント (2012 年 4 月) Google＋ユーザ： 1億人/月、5000 万人/日 (2012 年 3 月)	登録ユーザ：2700 人 ログインユーザ数： 1512 万人/月 (2012 年 3 月)	Hotmail：3.6 億アカウント	アクティブユーザ：2600 万人/月 有料会員：780 万人 (2012 年 3 末) メールユーザ数：1,750 万人(2010 年 11 月末) オンラインストレージ： 100 万人(2012 年 1 月)	登録ユーザ：1170 万人 (2012 年 3 月)	登録ユーザ：6,000 人 （プラットフォーム OpenSNP を利用している地域ＳＮＳに限る）
クラウドの運用状況	電子メール、ドキュメント作成、カレンダー、グループ、SNS などをクラウドで運用	イベント開催時にスケーラビリティ確保を目的として運用	電子メール、カレンダー、オンラインストレージ、オンラインフォトアルバムをクラウドで運用	電子メールおよびオンラインストレージをクラウドで運用	電子メール、ブログ、ベーシックホスティングなどほぼ全てのサービスをクラウドで運用	一部地域SNSがクラウドで運用
障害事例と影響	Gmail で障害、利用者の 10%に影響(2012 年)	1 日以上のサービス停止(2010 年)	日本国内の hotmail ユーザ 940 万人にアクセス障害(2010 年)		ココログに障害、縮退運用のため一部ユーザに 24 時間以上にわたってサービスの一部を制限	大きな障害の事例はない
震災時の対応	災害支援サービスを複数提供	災害関連情報交換を mixi コミュニティ上でユーザが自主的に実施、運営側もサーバを平常時よりも多く設置して急激なアクセス増加に対応		ウェブサイトの更新を 2 拠点で可能にし、震災特設ページで震災関連情報を発信	災害支援サービスを複数提供	震災直後に各コミュニティの情報交換の場として機能

1.2. 消費者向け電子商取引のシステム基盤としてのクラウド

1.2.1. 調査の概要

消費者向け電子商取引におけるクラウドコンピューティングの現状と課題の把握を行うために、アンケートを実施した。アンケートは、インターネットにより行い、モニターの中から電子商取引に知見を有する人（例：IT 担当、販売担当、マーケティング担当の方など）向けに依頼した。

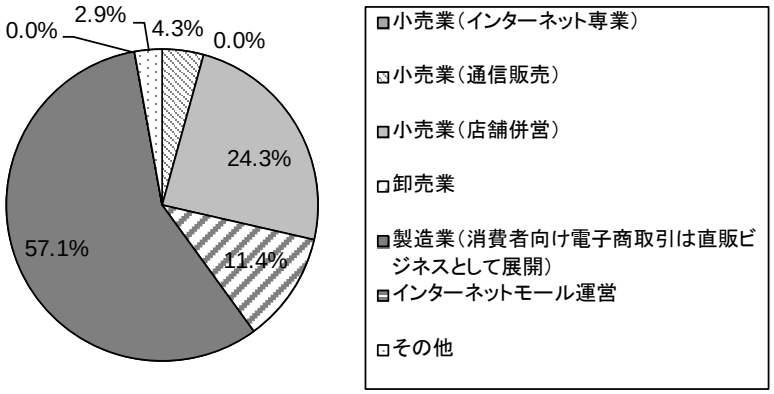
- 実施日時：2012 年 3 月 1 日～6 日
- 調査方法：インターネット上の調査母集団に対して回答資格の有無を判別するスクリーニング設問を行い、該当者のみに本調査を実施した。
- 回答数：70 サンプル
- 質問内容
  - ○ 消費者向け電子商取引の状況
    - ・ 店舗形態
    - ・ 売上規模、推移
    - ・ ユーザの状況　等
  - ○ 消費者向け電子商取引を支える技術、とりわけクラウドサービス
    - ・ システムの保有・利用形態
    - ・ クラウドを利用する理由
    - ・ クラウドを利用しない理由　等
  - ○ クラウド停止の影響
    - ・ クラウド停止の影響
    - ・ 停止等のリスクへの対策　等

1.2.2. アンケート集計結果

(1) 回答者の属性

70 の有効回答を得た。回答者の内訳としては、57%が製造業(消費者向け電子商取引は直販ビジネスとして展開)、小売業はインターネット専業、通信販売、店舗併営合わせて 29%であった。

図表 5 回答者の業種分布

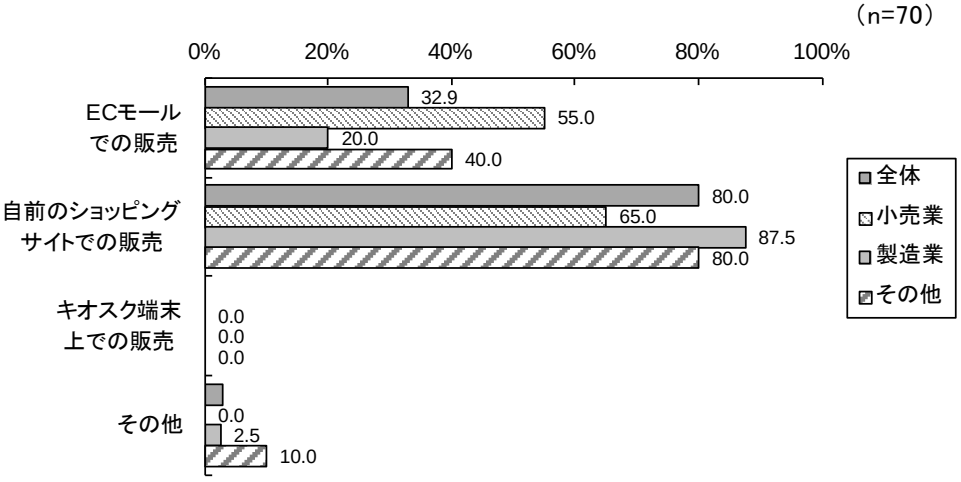


(2) 消費者向け電子商取引の状況

① 店舗形態

全体で見ると 80%が自前のサイト運営、EC モールは 33%である。業種別には小売業では EC モールでの出店が多く、製造業では自前のショッピングサイトでの販売が多い。

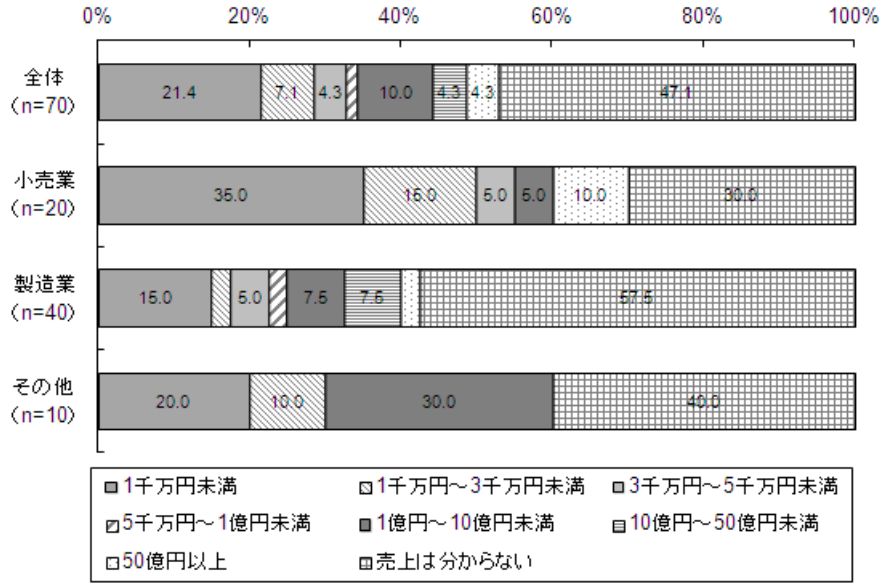
図表 6 インターネット上の店舗形態



② 売上規模

売上規模は 1 千万円未満が 21%、1 億円以上は 19%である。

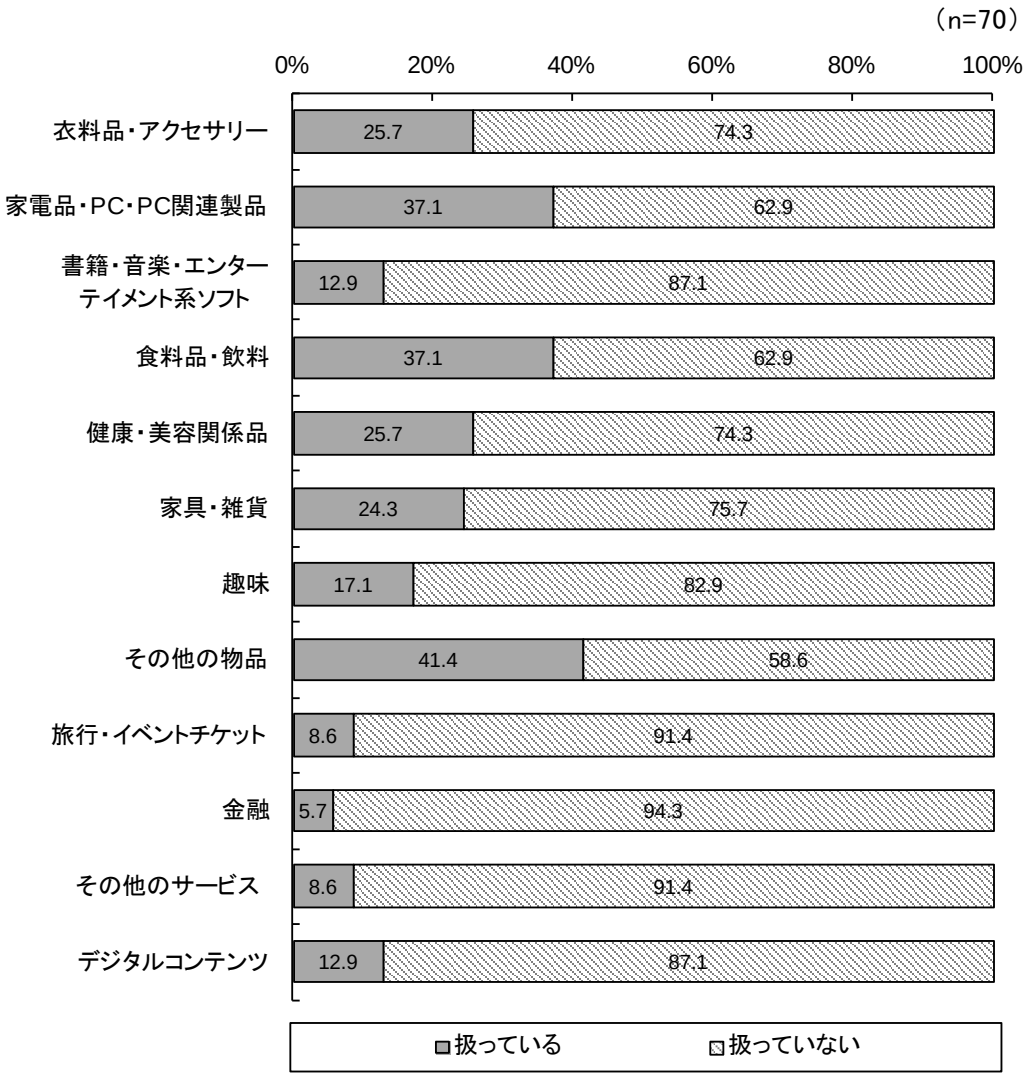
図表 7 消費者向け電子商取引の売上規模



③ 取り扱い品目

取り扱いが多い品目は、その他物品（41%）、食料品・飲料、家電品・PC・PC 関連製品（いずれも 37%）である。

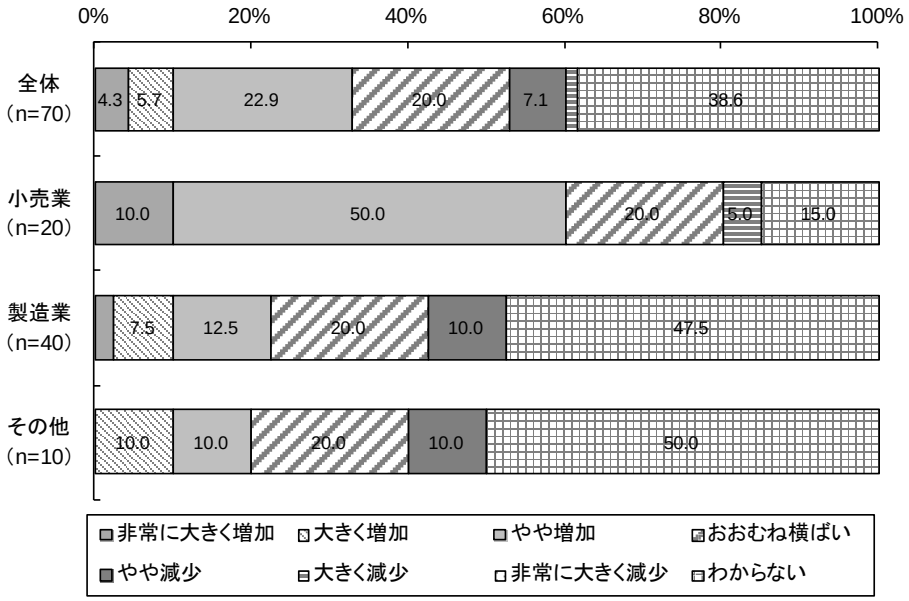
図表 8 消費者向けに電子商取引を行っている品目



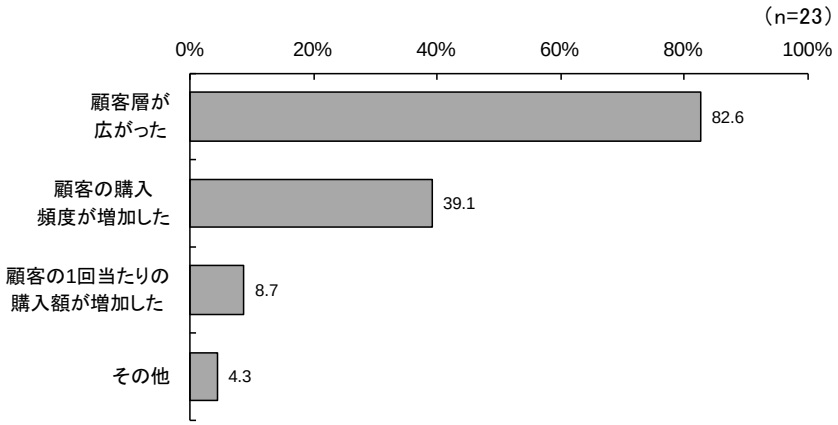
④ 売上の推移、背景

全体で見ると直近 3 か年では売上が増加している事業者が合わせて 33%、おおむね横ばいが 20%、減少しているは 9%であり、市場は拡大傾向にあると言える。売上増加の背景は、顧客層拡大を指摘した回答者が最も多い。その要因としては、時間短縮や品質、価格重視の顧客増が多く指摘されている。

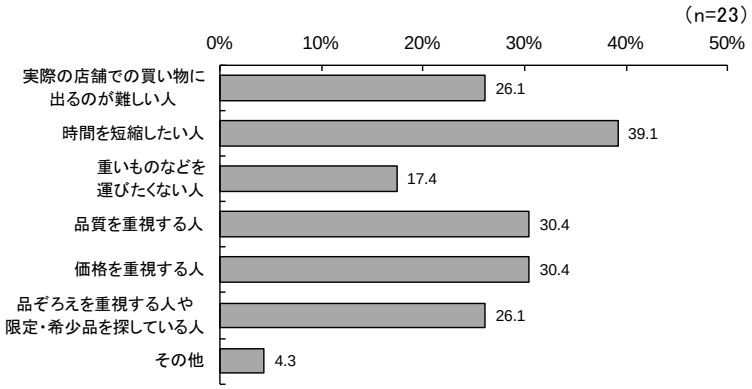
図表 9 消費者向け電子商取引の直近 3 カ年の推移



図表 10 電子商取引の売上増加の背景・要因



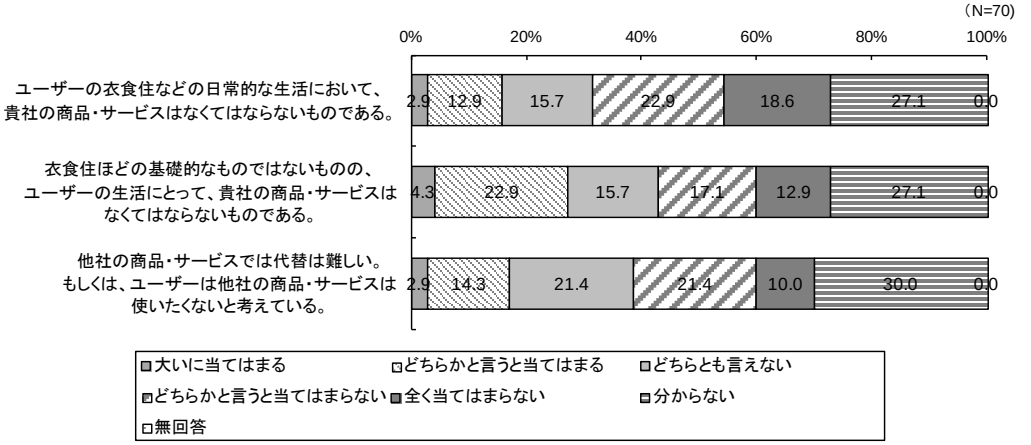
図表 11 電子商取引の売上増加の背景となった顧客層



⑤ ヘビーユーザーの認識

ヘビーユーザー[24]の考えについて、回答者の認識を聞いたところ、ヘビーユーザーにとって自社の商品・サービスが「日常的な生活に不可欠である」ととらえている回答者は約 16%、「衣食住ほどの基礎的なものではないもののユーザにとってなくてはならない」ととらえている回答者は約 27%と、43%が必需性について肯定的回答であった。

図表 12 ヘビーユーザーの認識



⑥ 今後の売上の見込み

自社の電子商取引について、44%以上の事業者が今後売上は増加すると回答しており、減少するとの予測は 5%程度である。とりわけ小売業において増加するとの回答は多い。

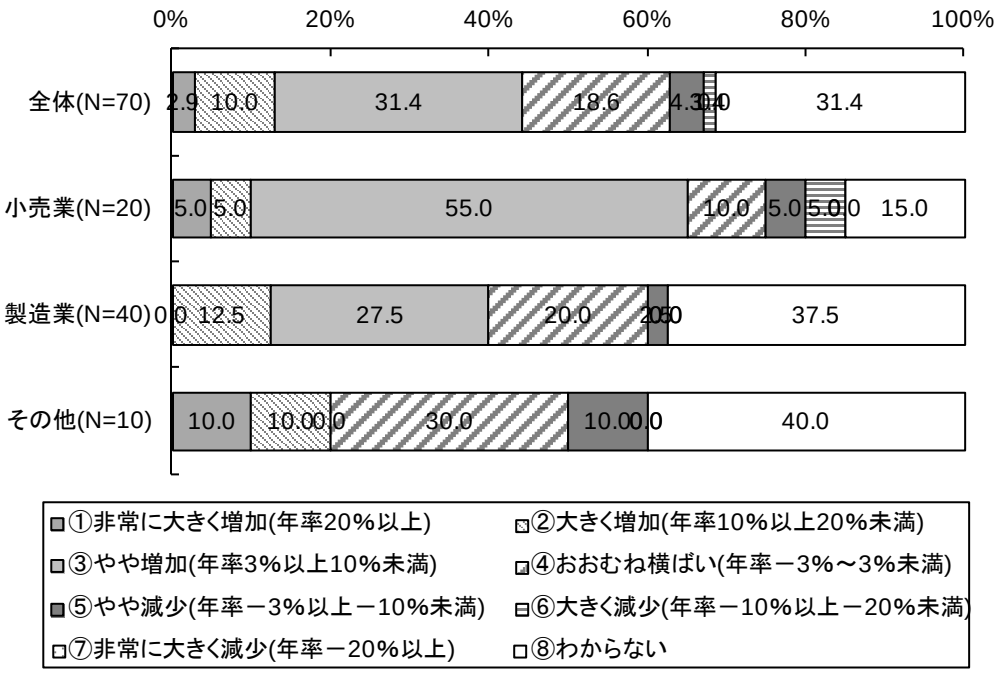
今後 3 年程度の電子商取引市場の売上の見込みについては、全体のうち約半数が日用的な食料品や介護・医薬品の EC 販売は増加すると予測している。また、

24 ヘビーユーザーとは、ここでは、顧客単価もしくは利用頻度が平均的な水準よりも高い顧客を指す。

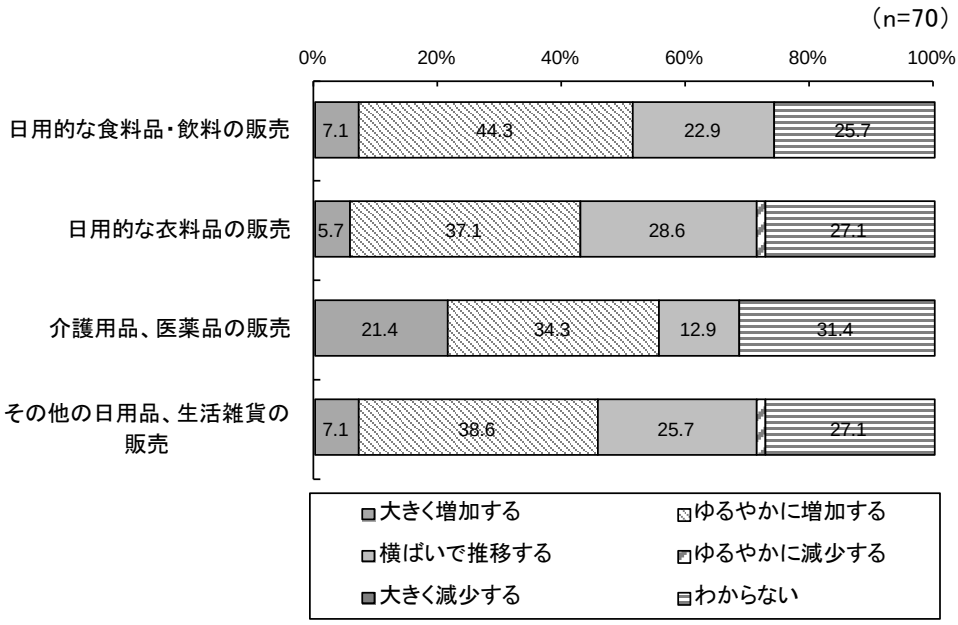
電子商取引市場の売上が増加すると考えた理由としては、高齢化の影響、また調べてから消費するユーザが増える傾向を指摘する回答が多かった。

これらのことから、現状では利用者にとっての重要度が高いとは言えないものの今後は利用の規模や重要度が高まっていくものと考えられる。

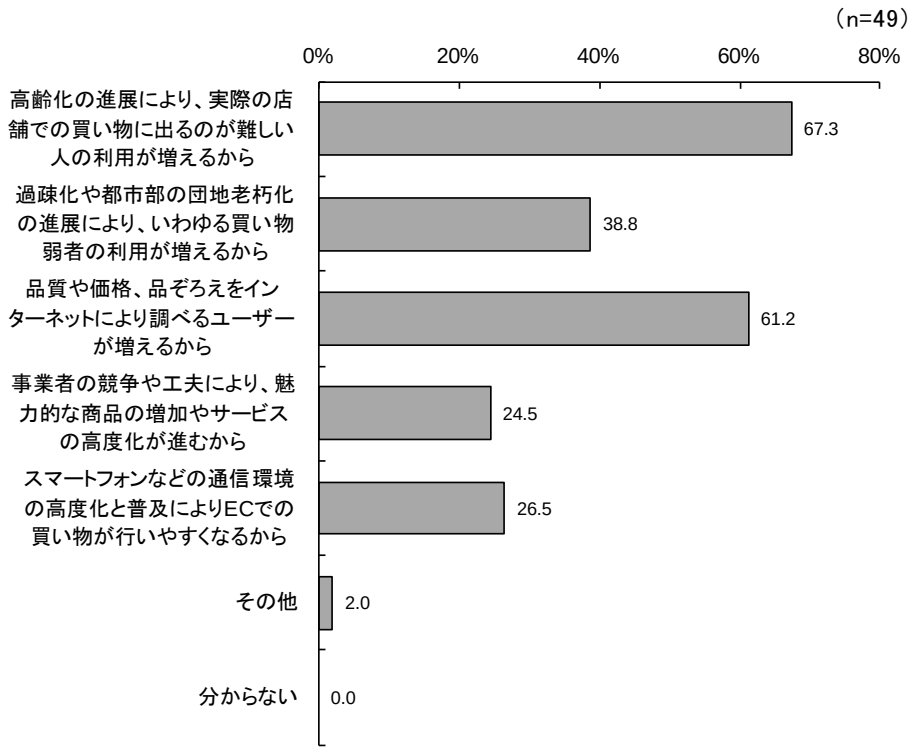
図表 13 今後 3 年程度の自社の電子商取引の売上の見込み



図表 14 今後 3 年程度の電子商取引市場の売上の見込み



図表 15 電子商取引の市場の売上が増加すると考えた理由

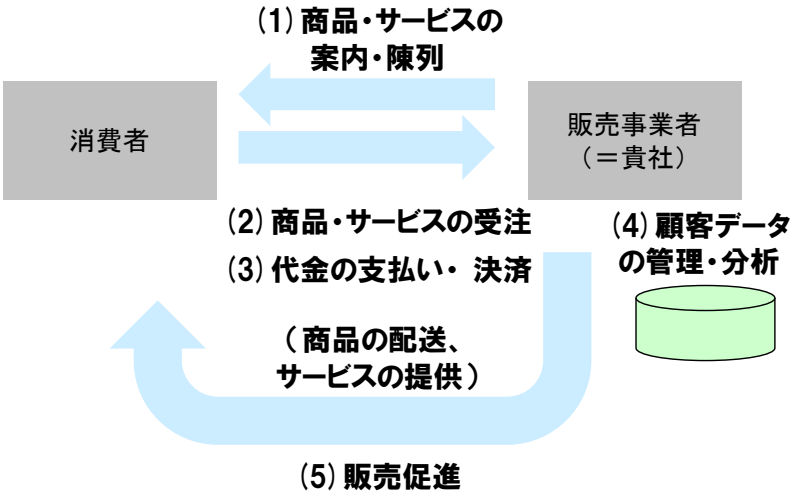


(3) 電子商取引を支える技術・クラウドについて

以下では、業務の種類別およびシステムのレイヤーごとにシステムの運用形態を質問し、クラウドの利用の傾向について把握する。

業務の種類は、電子商取引の業務を図表 16 のように分類し、またシステムのレイヤーを図表 17 のようにデータセンター、ハードウェアおよびネットワーク、OS およびプラットフォーム、アプリケーションと 4 つに分解した。

図表 16 本アンケートで用いた電子商取引の業務の分類



図表 17 本アンケートで用いたシステムレイヤーの分類

アプリケーション
OS、プラットフォーム
ハードウェア、ネットワーク
データセンター

① システムの保有・利用形態

商品サービスの案内・陳列でのアウトソース・外部利用が比較的多い。

顧客データの管理・分析はアウトソース・外部利用が少ない。クラウドを利用したくない業務（後述）としても、もっとも多い（約 25%が利用したくないと回答）。

小売業のほうが製造業と比べると、アウトソース・外部利用との回答割合がおおむね高い傾向にある。

図表 18 システムの保有・利用形態

全体

（n=70）

		①自社保有	②アウトソース・外部利用	①②の併用	利用していない・わからない
(1) 商品・サービスの案内・陳列	アプリケーション	52.9	20.0	7.1	20.0
	OS、プラットフォーム	51.4	20.0	5.7	22.9
	ハードウェア、ネットワーク	52.9	18.6	8.6	20.0
	データセンター	30.0	32.9	5.7	31.4
(2) 商品・サービスの受注	アプリケーション	50.0	18.6	10.0	21.4
	OS、プラットフォーム	50.0	20.0	7.1	22.9
	ハードウェア、ネットワーク	48.6	18.6	10.0	22.9
	データセンター	31.4	25.7	8.6	34.3
(3) 代金の支払い・決済	アプリケーション	42.9	18.6	5.7	32.9
	OS、プラットフォーム	40.0	18.6	5.7	35.7
	ハードウェア、ネットワーク	41.4	15.7	7.1	35.7
	データセンター	28.6	22.9	5.7	42.9
(4) 顧客データの管理・分析（ログ解析、顧客の声の分析など）	アプリケーション	50.0	10.0	7.1	32.9
	OS、プラットフォーム	44.3	15.7	8.6	31.4
	ハードウェア、ネットワーク	44.3	15.7	8.6	31.4
	データセンター	34.3	15.7	4.3	45.7
(5) 販売促進（ITシステムを活用した広告、レコメンデーションなど）	アプリケーション	32.9	12.9	11.4	42.9
	OS、プラットフォーム	32.9	14.3	8.6	44.3
	ハードウェア、ネットワーク	35.7	12.9	7.1	44.3
	データセンター	25.7	18.6	5.7	50.0

小売業

（n=20）

		①自社保有	②アウトソース・外部利用	①②の併用	利用していない・わからない
(1) 商品・サービスの案内・陳列	アプリケーション	30.0	30.0	10.0	30.0
	OS、プラットフォーム	30.0	25.0	10.0	35.0
	ハードウェア、ネットワーク	30.0	30.0	15.0	25.0
	データセンター	25.0	25.0	10.0	40.0
(2) 商品・サービスの受注	アプリケーション	30.0	25.0	15.0	30.0
	OS、プラットフォーム	30.0	20.0	15.0	35.0
	ハードウェア、ネットワーク	25.0	25.0	15.0	35.0
	データセンター	25.0	20.0	10.0	45.0
(3) 代金の支払い・決済	アプリケーション	25.0	25.0	10.0	40.0
	OS、プラットフォーム	20.0	20.0	15.0	45.0
	ハードウェア、ネットワーク	20.0	25.0	10.0	45.0
	データセンター	15.0	20.0	10.0	55.0
(4) 顧客データの管理・分析（ログ解析、顧客の声の分析など）	アプリケーション	35.0	10.0	15.0	40.0
	OS、プラットフォーム	25.0	20.0	15.0	40.0
	ハードウェア、ネットワーク	20.0	25.0	15.0	40.0
	データセンター	25.0	10.0	10.0	55.0
(5) 販売促進（ITシステムを活用した広告、レコメンデーションなど）	アプリケーション	15.0	15.0	15.0	55.0
	OS、プラットフォーム	10.0	20.0	15.0	55.0
	ハードウェア、ネットワーク	20.0	15.0	10.0	55.0
	データセンター	20.0	10.0	10.0	60.0

製造業

（n=40）

		①自社保有	②アウトソース・外部利用	①②の併用	利用していない・わからない
(1) 商品・サービスの案内・陳列	アプリケーション	62.5	15.0	5.0	17.5
	OS、プラットフォーム	60.0	20.0	2.5	17.5
	ハードウェア、ネットワーク	62.5	15.0	5.0	17.5
	データセンター	37.5	30.0	5.0	27.5
(2) 商品・サービスの受注	アプリケーション	65.0	12.5	5.0	17.5
	OS、プラットフォーム	62.5	17.5	2.5	17.5
	ハードウェア、ネットワーク	62.5	15.0	5.0	17.5
	データセンター	40.0	22.5	7.5	30.0
(3) 代金の支払い・決済	アプリケーション	57.5	12.5	0.0	30.0
	OS、プラットフォーム	52.5	15.0	0.0	32.5
	ハードウェア、ネットワーク	55.0	10.0	2.5	32.5
	データセンター	40.0	20.0	2.5	37.5
(4) 顧客データの管理・分析（ログ解析、顧客の声の分析など）	アプリケーション	65.0	5.0	0.0	30.0
	OS、プラットフォーム	57.5	10.0	5.0	27.5
	ハードウェア、ネットワーク	60.0	10.0	2.5	27.5
	データセンター	45.0	12.5	0.0	42.5
(5) 販売促進（ITシステムを活用した広告、レコメンデーションなど）	アプリケーション	45.0	12.5	5.0	37.5
	OS、プラットフォーム	45.0	12.5	2.5	40.0
	ハードウェア、ネットワーク	45.0	12.5	2.5	40.0
	データセンター	32.5	20.0	0.0	47.5

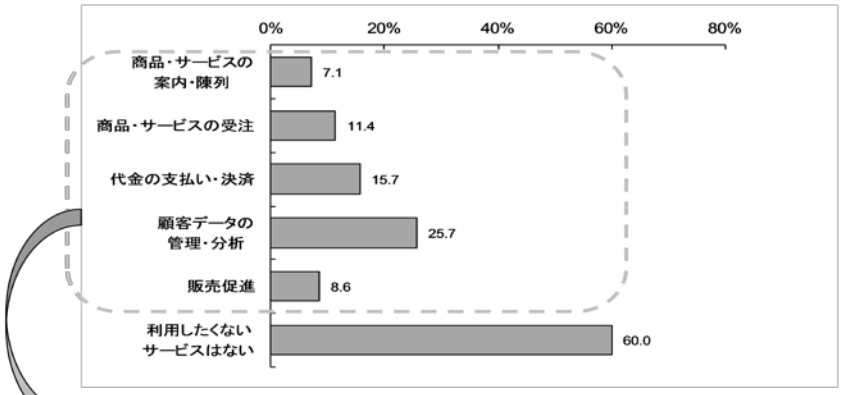
② クラウド利用の理由

システムコスト（開発・運用）の節減が最も強い理由であり、次いで、安定したシステム稼働との回答が多い。クラウドを利用したくない業務としては顧客データの管理・分析が最も多く、これはセキュリティへの不安が大きく影響している。サービスの安定性に不安との回答も 28%弱に上る。

図表 19 クラウドを利用した理由

		システムコスト（開発・運用）の節減	将来の業務量増加への対応（スケーラビリティの確保）	高度なシステム機能への対応	システムの利用開始までの時間の短さ	自社のIT人材の不足を外部サービスで補う	安定したシステム稼働	災害時等の業務継続が容易	自社システムより情報セキュリティが確保しやすい	取引先の要請	その他
(1) 商品・サービスの案内・陳列 (n=38)	クラウド導入の理由	63.2	21.1	15.8	23.7	21.1	34.2	15.8	23.7	2.6	7.9
	もっとも強い理由	52.6	5.3	0.0	5.3	2.6	15.8	2.6	7.9	0.0	7.9
(2) 商品・サービスの受注 (n=35)	クラウド導入の理由	65.7	28.6	17.1	25.7	28.6	22.9	14.3	14.3	5.7	8.6
	もっとも強い理由	42.9	8.6	2.9	8.6	8.6	14.3	2.9	0.0	2.9	8.6
(3) 代金の支払い・決済 (n=28)	クラウド導入の理由	64.3	17.9	21.4	21.4	17.9	25.0	10.7	14.3	7.1	7.1
	もっとも強い理由	46.4	0.0	3.6	7.1	7.1	17.9	0.0	7.1	0.0	7.1
(4) 顧客データの管理・分析（ログ解析、顧客の声の分析など) (n=25)	クラウド導入の理由	72.0	40.0	16.0	12.0	20.0	24.0	12.0	12.0	4.0	4.0
	もっとも強い理由	60.0	8.0	4.0	4.0	4.0	8.0	4.0	4.0	0.0	4.0
(5) 販売促進（ITシステムを活用した広告、レコメンデーションなど) (n=24)	クラウド導入の理由	75.0	29.2	33.3	33.3	8.3	33.3	8.3	16.7	4.2	0.0
	もっとも強い理由	54.2	0.0	12.5	8.3	0.0	20.8	0.0	4.2	0.0	0.0

図表 20 クラウドなど他社保有のシステム・サービスを利用できない・したくない業務、その理由



		情報セキュリティに不安があるから	サービスの安定性に不安があるから	利用のコストが見合わないから	適切なサービスがないから	現行システムで十分だから	現行システムからの移行が困難だから	その他
商品・サービスの案内・陳列	(n=5)	20.0	60.0	20.0	20.0	0.0	0.0	0.0
商品・サービスの受注	(n=8)	25.0	25.0	25.0	12.5	12.5	12.5	0.0
代金の支払い・決済	(n=11)	27.3	27.3	9.1	9.1	9.1	9.1	9.1
顧客データの管理・分析	(n=18)	77.8	27.8	16.7	0.0	5.6	5.6	0.0
販売促進	(n=6)	50.0	16.7	16.7	33.3	0.0	0.0	0.0

(4) クラウド停止の影響

① 停止時の業務への影響

各業務について、事業者の約 50～60%が継続できると回答している。有効回答数(N)が少なく、また業務により異なるため、単純に比較はできないものの、停止期間 1 日程度の場合、小売業では約半数が「代替手段はなく業務の継続は困難となる」または「業務の一部に継続できないものが生じる」と回答しているのに対して、製造業では同回答の割合は 30～40%前後である。

図表 21 大規模災害等で仮にクラウドが停止してしまった場合の、自社業務への影響

全体
【停止期間1日程度】

	代替手段はなく業務の継続は困難となる	業務の一部に継続できないものが生じる	すべての業務は継続できるが業務処理の能力が低下する	すべての業務は継続できるが代替手段確保に経済的な負担が発生する	大きな支障なくすべての業務が継続できる	その他
商品・サービスの案内・陳列 (n=38)	15.8	21.1	34.2	2.6	26.3	0.0
商品・サービスの受注 (n=35)	17.1	28.6	31.4	2.9	20.0	0.0
代金の支払い・決済 (n=28)	14.3	35.7	25.0	7.1	17.9	0.0
顧客データの管理・分析 (n=25)	8.0	40.0	32.0	8.0	12.0	0.0
販売促進 (n=24)	12.5	25.0	33.3	8.3	20.8	0.0

【停止期間3日程度】

	代替手段はなく業務の継続は困難となる	業務の一部に継続できないものが生じる	すべての業務は継続できるが業務処理の能力が低下する	すべての業務は継続できるが代替手段確保に経済的な負担が発生する	大きな支障なくすべての業務が継続できる	その他
商品・サービスの案内・陳列 (n=38)	18.4	23.7	28.9	7.9	21.1	0.0
商品・サービスの受注 (n=35)	14.3	37.1	20.0	14.3	14.3	0.0
代金の支払い・決済 (n=28)	17.9	28.6	17.9	21.4	14.3	0.0
顧客データの管理・分析 (n=25)	16.0	36.0	20.0	16.0	12.0	0.0
販売促進 (n=24)	16.7	29.2	20.8	12.5	20.8	0.0

小売業
【停止期間1日程度】

	代替手段はなく業務の継続は困難となる	業務の一部に継続できないものが生じる	すべての業務は継続できるが業務処理の能力が低下する	すべての業務は継続できるが代替手段確保に経済的な負担が発生する	大きな支障なくすべての業務が継続できる	その他
商品・サービスの案内・陳列 (n=13)	7.7	38.5	38.5	0.0	15.4	0.0
商品・サービスの受注 (n=11)	9.1	54.5	18.2	0.0	18.2	0.0
代金の支払い・決済 (n=10)	0.0	50.0	20.0	0.0	30.0	0.0
顧客データの管理・分析 (n=9)	0.0	44.4	33.3	11.1	11.1	0.0
販売促進 (n=7)	0.0	57.1	28.6	0.0	14.3	0.0

【停止期間3日程度】

	代替手段はなく業務の継続は困難となる	業務の一部に継続できないものが生じる	すべての業務は継続できるが業務処理の能力が低下する	すべての業務は継続できるが代替手段確保に経済的な負担が発生する	大きな支障なくすべての業務が継続できる	その他
商品・サービスの案内・陳列 (n=13)	23.1	38.5	23.1	0.0	15.4	0.0
商品・サービスの受注 (n=11)	9.1	63.6	0.0	9.1	18.2	0.0
代金の支払い・決済 (n=10)	10.0	50.0	10.0	0.0	30.0	0.0
顧客データの管理・分析 (n=9)	11.1	55.6	11.1	11.1	11.1	0.0
販売促進 (n=7)	14.3	57.1	14.3	0.0	14.3	0.0

製造業

【停止期間1日程度】

	代替手段はなく業務の継続は困難となる	業務の一部に継続できないものが生じる	すべての業務は継続できるが業務処理の能力が低下する	すべての業務は継続できるが代替手段確保に経済的な負担が発生する	大きな支障なくすべての業務が継続できる	その他
商品・サービスの案内・陳列 (n=16)	12.5	12.5	31.3	6.3	37.5	0.0
商品・サービスの受注 (n=16)	18.8	12.5	37.5	6.3	25.0	0.0
代金の支払い・決済 (n=11)	18.2	27.3	27.3	18.2	9.1	0.0
顧客データの管理・分析 (n=9)	11.1	33.3	33.3	11.1	11.1	0.0
販売促進 (n=11)	18.2	9.1	27.3	18.2	27.3	0.0

【停止期間3日程度】

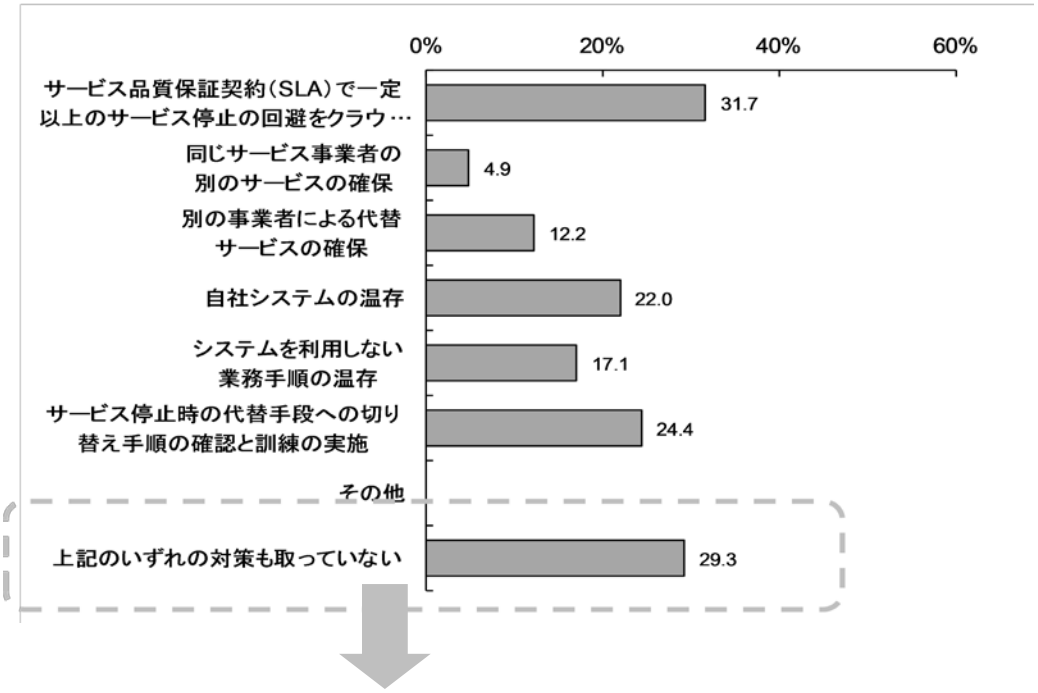
	代替手段はなく業務の継続は困難となる	業務の一部に継続できないものが生じる	すべての業務は継続できるが業務処理の能力が低下する	すべての業務は継続できるが代替手段確保に経済的な負担が発生する	大きな支障なくすべての業務が継続できる	その他
商品・サービスの案内・陳列 (n=16)	6.3	18.8	25.0	18.8	31.3	0.0
商品・サービスの受注 (n=16)	12.5	25.0	25.0	25.0	12.5	0.0
代金の支払い・決済 (n=11)	18.2	9.1	18.2	54.5	0.0	0.0
顧客データの管理・分析 (n=9)	11.1	22.2	22.2	33.3	11.1	0.0
販売促進 (n=11)	18.2	18.2	9.1	27.3	27.3	0.0

② 停止等のリスクへの対策

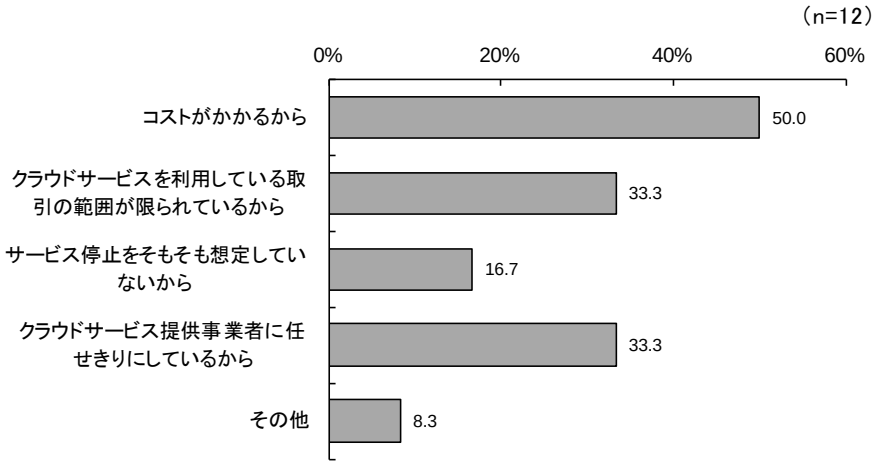
クラウド停止等のリスクへの対策としては、SLA、代替手段への切り替え、自社システム温存が多い。

対策を取っていない事業者も全体の約 30%に上っている。対策をとっていない理由としては、コストの問題やクラウド事業者に任せきりとの回答が多い。

図表 22 クラウド利用において、サービス停止等のリスクに対応するための対策



図表 23 対策をとっていない理由

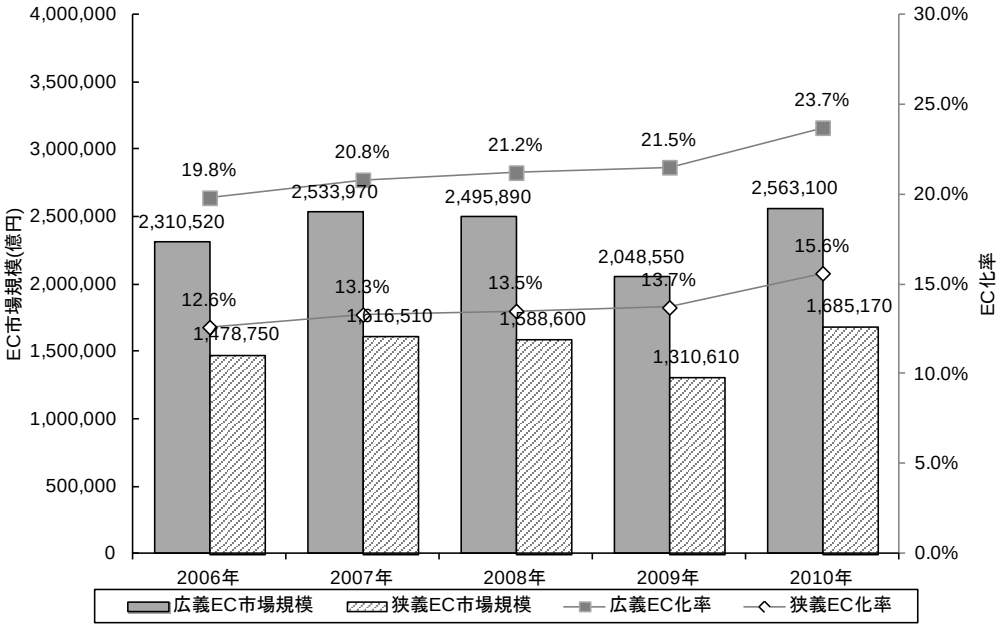


1.2.3. クラウドの浸透実態と課題

アンケート調査から明らかになったことを整理する。まず、クラウドに限らないが、消費者向け電子商取引は拡大している。図表 9 に示したように、直近 3 か年で売上高が増加していると認識する事業者が 33%、おおむね横ばいが 20%、減少しているは 9%であった。

この傾向は経済産業省「電子商取引に関する市場調査」（平成 23 年 2 月）においても確認できる。

図表 24 EC市場規模の推移 [25]



出所）経済産業省「電子商取引に関する市場調査」（平成 23 年 2 月）

本調査のアンケートでは、40%以上の事業者が今後売上は増加すると回答、減少するとの予測は 5%程度であった。日用的な食料品や介護・医薬品を中心に、今後 EC の利用は増加することが予想される。

このように EC の市場が増大するなか、EC のシステムにもクラウドが活用されているところは多く、クラウドの社会への浸透が B2C においても徐々に広がっているということができる。アンケートでは、システム開発・運用コストの縮減などを目的に、商品サービスの案内等においてアウトソース・外部利用があることがわかった。

---

25 広義の EC：コンピューターネットワークシステムを介して商取引（受発注）が行われ、かつその成約金額が捕捉されるもの。
狭義の EC：インターネット技術を用いた、コンピューターネットワークシステムを介して商取引（受発注）が行われ、かつその成約金額が捕捉されるもの。

他方、顧客データの管理・分析という業務については、アウトソース・外部利用が少ない。クラウドを利用したくない業務としても、もっとも多く、約 25%の事業者が「利用したくない」と回答している。顧客データ関係のクラウド利用がない理由としては、「情報セキュリティに不安がある」が約 80%に上り、他の業務や他の理由と比べても特徴的である。B2C においては、大量の顧客データとその活用が企業の競争力を左右したり、企業に対する顧客の信頼性の観点からクリティカルであったりすることが多く、クラウド化すると、場合によっては自社のコントールが効きにくくなる可能性が生じることに慎重な事業者も多いことが推察される。

クラウドが万一停止してしまった場合については、50～60%の事業者が「継続できる」と回答しているものの、「一部の顧客に深刻な影響がある」との回答も 45%に上り、クラウドの停止が社会に対して大きな影響を与える可能性が高いことが示唆された。

クラウド停止等のリスクに備えては、SLA、代替手段への切り替え、自社システム温存という対策を講じている事業者が多い半面、対策を取っていないという事業者も約 30%に上る。クラウド事業者に任せきりとしているユーザ企業も多いことが伺われる。

1.3. 企業の生産販売、企業間情報連携等の情報インフラとしてのクラウド

1.3.1. 調査の概要

企業の生産販売ならびに受発注を初めとするサプライチェーンマネジメントを支える情報インフラとしてのクラウドコンピューティングの現状と課題の把握を行うために、アンケートを実施した。アンケートは、インターネットにより行い、モニターの中から、製造業、卸売業ならびに小売業に勤務し、かつ生産販売またはそれに関わる情報システムに知見を有する人(例:IT 担当、生産販売管理業務等の従事者)に回答を依頼した。

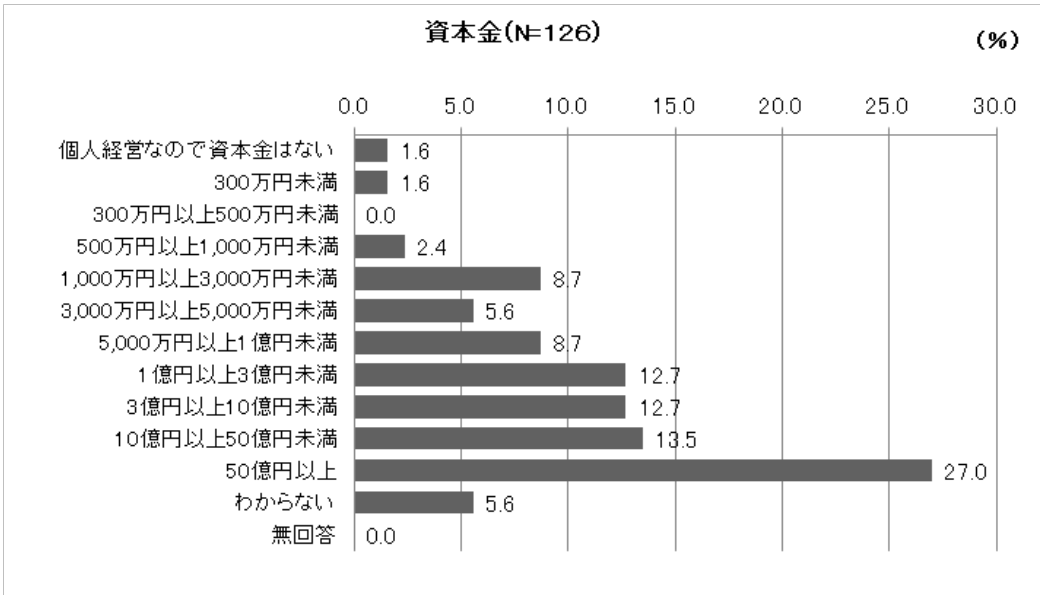
- 実施日時:2012 年 3 月 1 日～6 日
- 調査方法:インターネット上の調査母集団に対して回答資格の有無を判別するスクリーニング設問を行い、該当者のみに本調査を実施した。
- 回答数:126 サンプル
- 質問内容
  - ○ 回答者の属性
    - ・ 回答者勤務先の属性:業種、規模(資本金、従業員、売上)
    - ・ 勤務先で行っている業務種類
  - ○ 勤務先企業が行っている業務ごとのクラウドの利用実態
    - ・ 行っている業務種類ごとのコンピュータ利用の有無
    - ・ 行っている業務種類ごとのクラウド利用の有無と利用形態
    - ・ 行っている業務種類ごとのクラウド利用の動機
    - ・ クラウド利用ができない業務とその理由
  - ○ クラウド停止の場合に想定される影響とそれに向けた対応
    - ・ クラウド停止に伴う業務への影響(停止期間 1 日及び 3 日を想定)
    - ・ クラウド停止リスクへの対応の有無と種類
    - ・ クラウド停止リスクへの対応に対する懸念
    - ・ クラウド停止リスクへの対応を行っていない理由

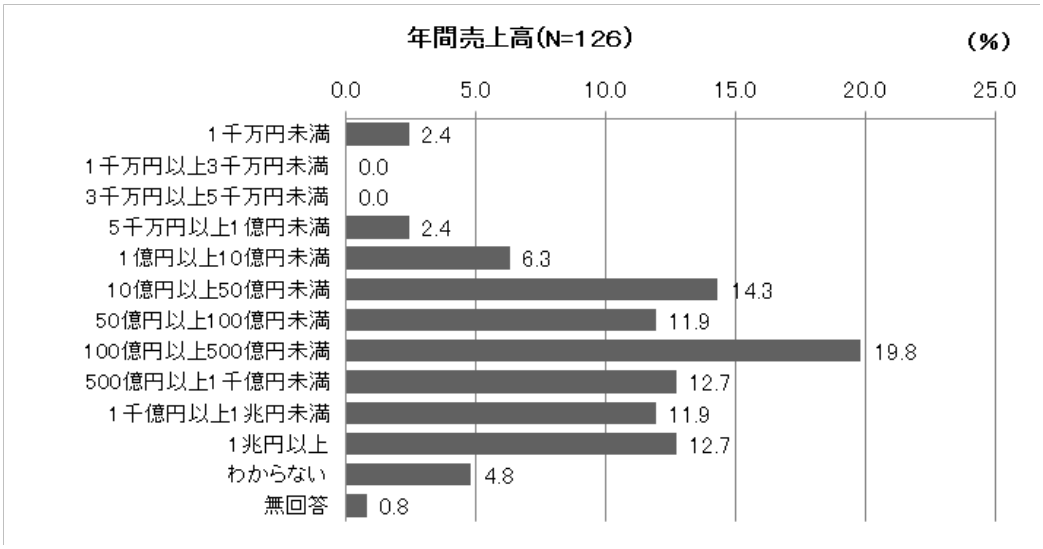
1.3.2. アンケート集計結果

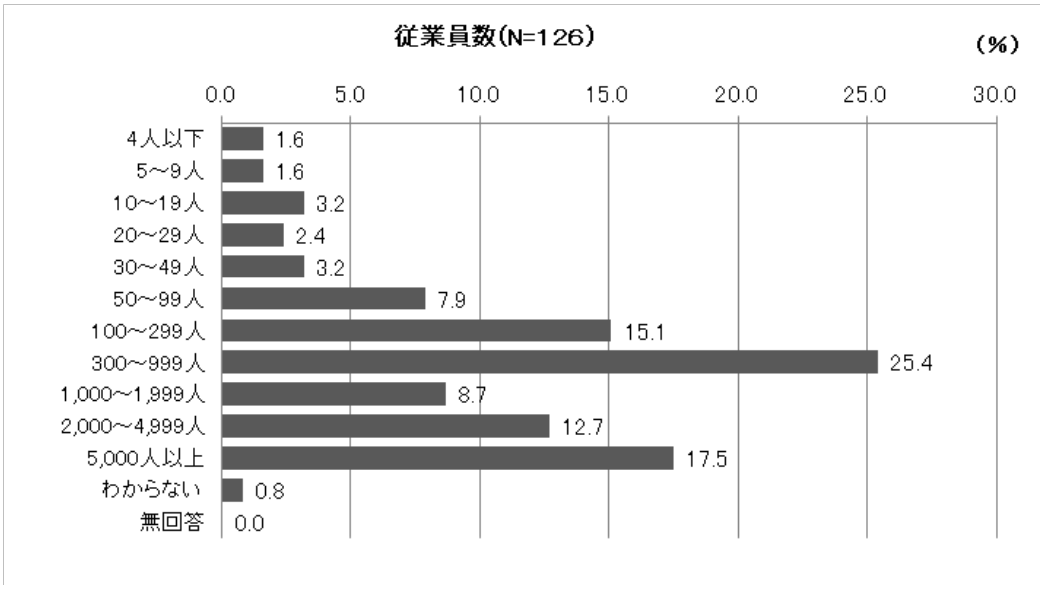
(1) 回答者の属性

回答者の所属企業は、「50 億円以上」が 27%、「10 億円以上 50 億円未満」を含めると 40.5%となっており、比較的大手企業に勤務する回答者からの情報が多く得られた。

図表 25 回答者の勤務先企業の属性

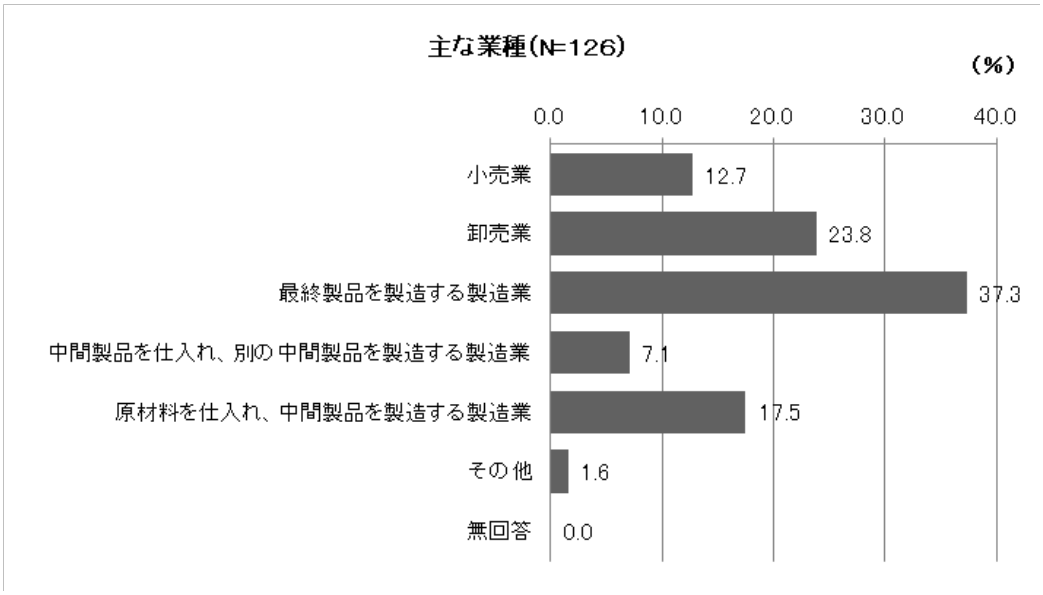






業種としては、「最終製品を製造する製造業」や「卸売業」など、サプライチェーンの下流に位置する企業に勤務する回答者が多く、サプライチェーンの中間に位置すると考えられる「中間製品を仕入れ、別の中間製品を製造する製造業」は 7.1%と少なかった。

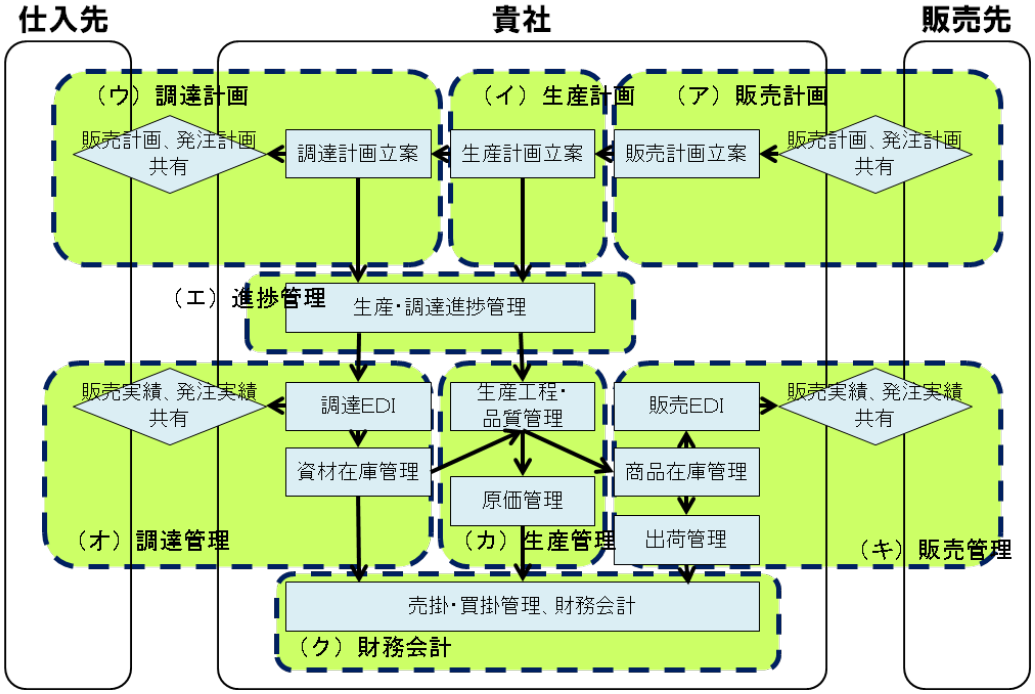
図表 26 回答者の勤務先企業のサプライチェーンにおける位置



(2) 行っている業務

勤務先の企業が行っている業務を企業の生産販売等の機能によって下図(ア)～(ク)の 8 種類に分類した。

図表 27 業務分類

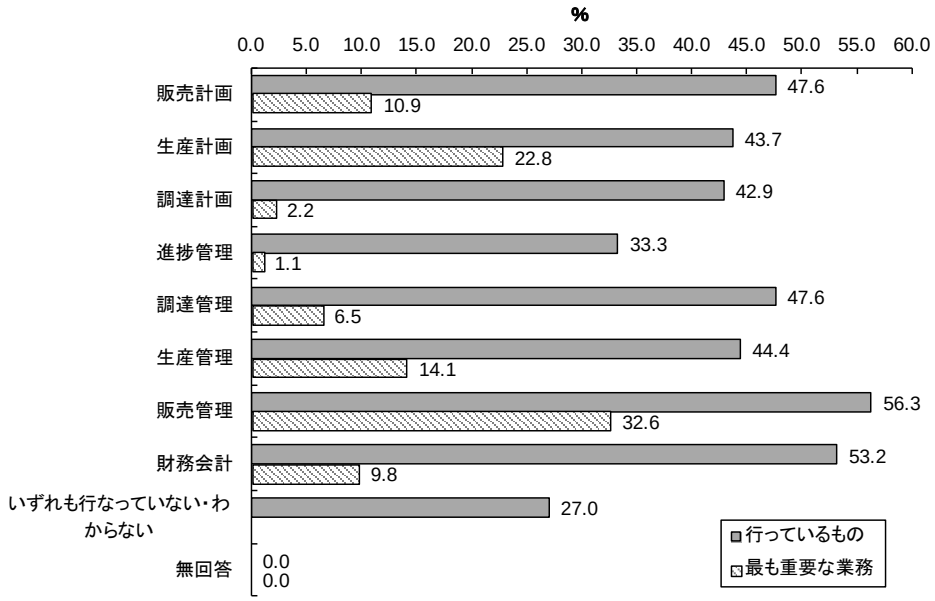


以下の設問では、この区分に従って業務の詳細やクラウドの利用について尋ねている。

勤務先の企業が行っている業務を上げてもらったところ、販売管理、財務会計、販売計画、調達管理、生産管理の順に多くなっている。ただし最も重要な業務を一つ選んでもらうと、販売管理が 30%以上と最も多く、次いで生産計画(22.8%)となっている。

取り組む業務は当然幅広いが、生産計画や販売の実情を知ることが重要な業務であると考えられている。

図表 28 回答者が勤務する企業で行っている業務および重要と考える業務(N=126)



最も重要な業務を回答者の業種別に見てみると、小売業・卸売業では販売管理、製造業では一般に生産計画が多くなっている。ただし、製造業もサプライチェーン上の位置によって傾向が異なっており、原材料を仕入れて中間製品を製造する製造業では生産計画よりも生産管理が最も重要とする回答が多かった。

図表 29 業種ごとの「重要と考える業務」

	回答者数	販売計画	生産計画	調達計画	進捗管理	調達管理	生産管理	販売管理	財務会計	無回答
小売業	10	20.0	0.0	0.0	0.0	0.0	0.0	80.0	0.0	0.0
卸売業	20	10.0	10.0	0.0	0.0	5.0	5.0	65.0	5.0	0.0
最終製品を製造する製造業	39	7.7	30.8	5.1	0.0	10.3	12.8	15.4	17.9	0.0
中間製品を仕入れ、別の中間製品を製造する製造業	6	0.0	50.0	0.0	0.0	16.7	16.7	16.7	0.0	0.0
原材料を仕入れ、中間製品を製造する製造業	17	17.6	23.5	0.0	5.9	0.0	35.3	11.8	5.9	0.0
その他	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

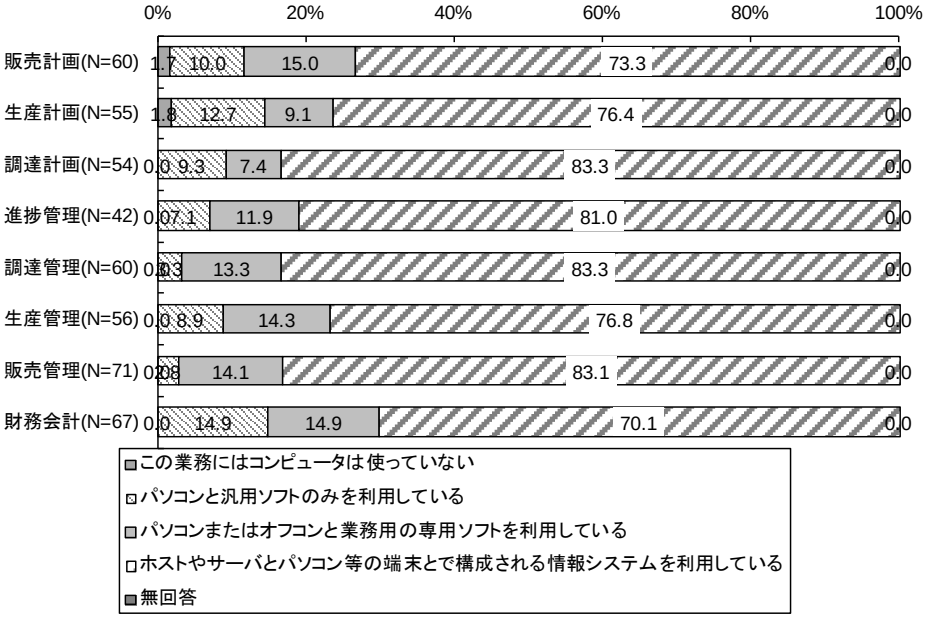
(3) 業務へのコンピュータ利用の有無と利用形態

業務ごとにコンピュータ利用の有無を尋ねたところ、ほとんどの業務において「ホストやサーバとパソコン等の端末とで構成される情報システムを利用している」としているものが最も多くなっている。

業務別の特徴は以下の通りである。

- 販売計画や生産計画ではコンピュータを利用しないとするものが少数ながら残っている。また、「パソコンと汎用ソフトのみ」「パソコンまたはオフコンと業務用の専用ソフト」の利用も比率としては大きい。
- 調達管理、販売管理では「パソコンまたはオフコンと業務用の専用ソフト」の利用の比率が大きく、「パソコンと汎用ソフトのみ」は少ない。
- 生産管理、財務会計では「パソコンと汎用ソフト」「パソコンまたはオフコンと業務用の専用ソフト」の利用が多い。

図表 30 業務へのコンピュータ利用の有無と利用形態



(4) 業務別のクラウド利用の傾向

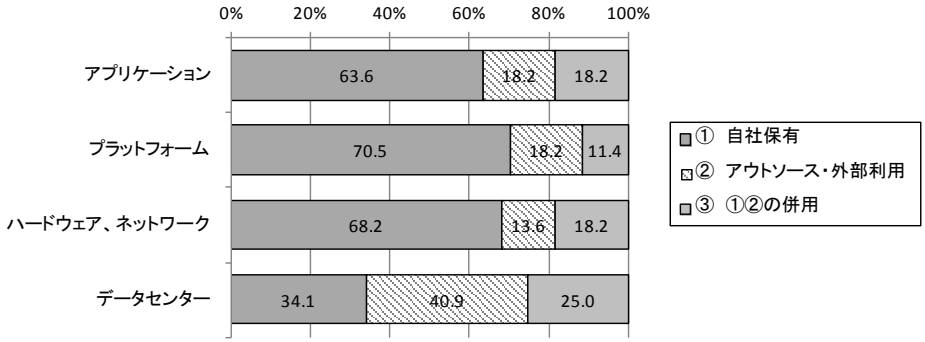
以下では、図表 27 に示した業務の種類別およびシステムをデータセンター、ハードウェアおよびネットワーク、プラットフォーム、アプリケーションと 4 つのレイヤーに分解し、そのレイヤーごとにシステムの運用形態を質問し、クラウドの利用の傾向について把握する。

① 販売計画

データセンターでは 41%が完全に外部化、25%が併用になっており、自社で運用しているものは 34%にとどまる。しかしながら、アプリケーション、プラットフォーム、ハードウェア・ネットワークにおいては、60～70%が自社保有となっている。その中でも、アプリケーションについてはやや自社保有の比率が小さくなっている。

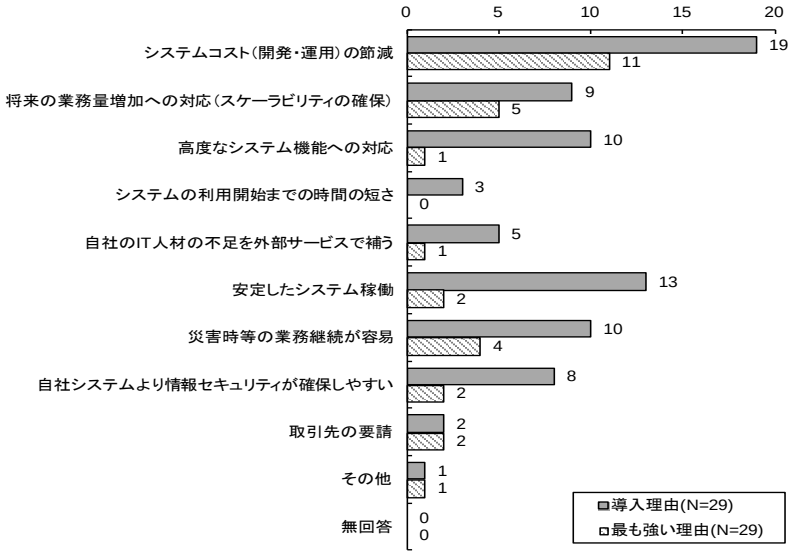
今回調査対象とした８業務の中では、データセンターの自社保有比率が最も低くなっている。

図表 31 システム利用形態・販売計画（N=44）



また、クラウド導入の理由として最も多いのは、「システムコストの節減」、次いで「安定した稼働」、「業務継続」、「高度システム機能への対応」であった。そのうち最も強い理由は「システムコストの節減」で、「将来の業務量増加への対応」がそれに次ぐ。

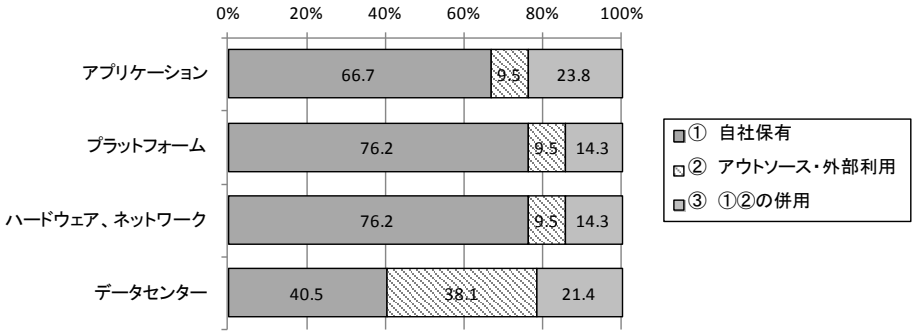
図表 32 クラウド導入の理由（販売計画）



② 生産計画

全体的な傾向は、データセンターでは外部利用や自社保有との併用が多いものの、ハードウェア・ネットワーク、プラットフォーム、アプリケーションにおいては 60～70%が自社保有している。これは販売計画と傾向が類似している。販売計画と比較すると、全体に自社保有の比率が高く、アウトソース・外部利用の比率が低くなっている。

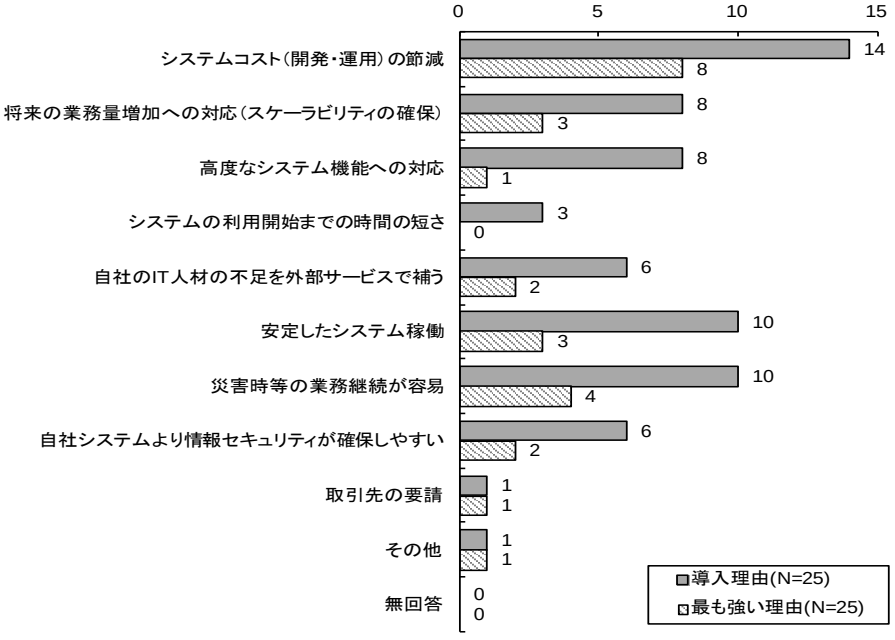
図表 33 システム利用形態・生産計画（N=42）



クラウド導入の理由は、「システムコストの節減」、「安定したシステム稼働」、「災害時の業務継続が容易」という順番に多い。「将来の業務量増加への対応」、「高度なシステム機能への対応」が他の業務に比べて多くなっていることが特徴的である。

最も強い理由は「システムコストの節減」、次いで「災害時等の業務継続が容易」が続く。

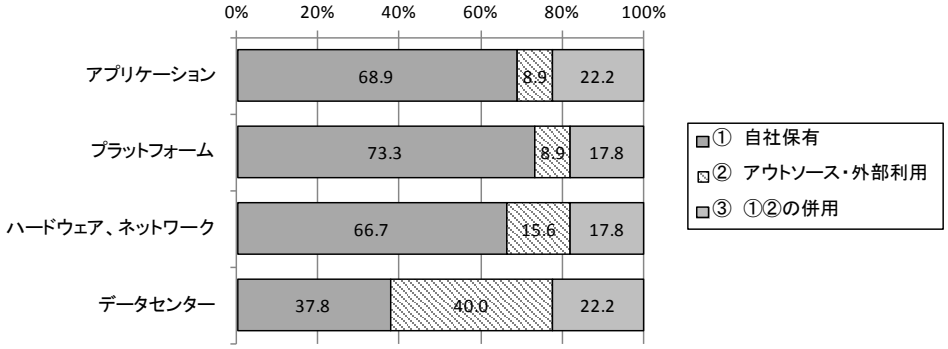
図表 34 クラウド導入の理由（生産計画）



③ 調達計画

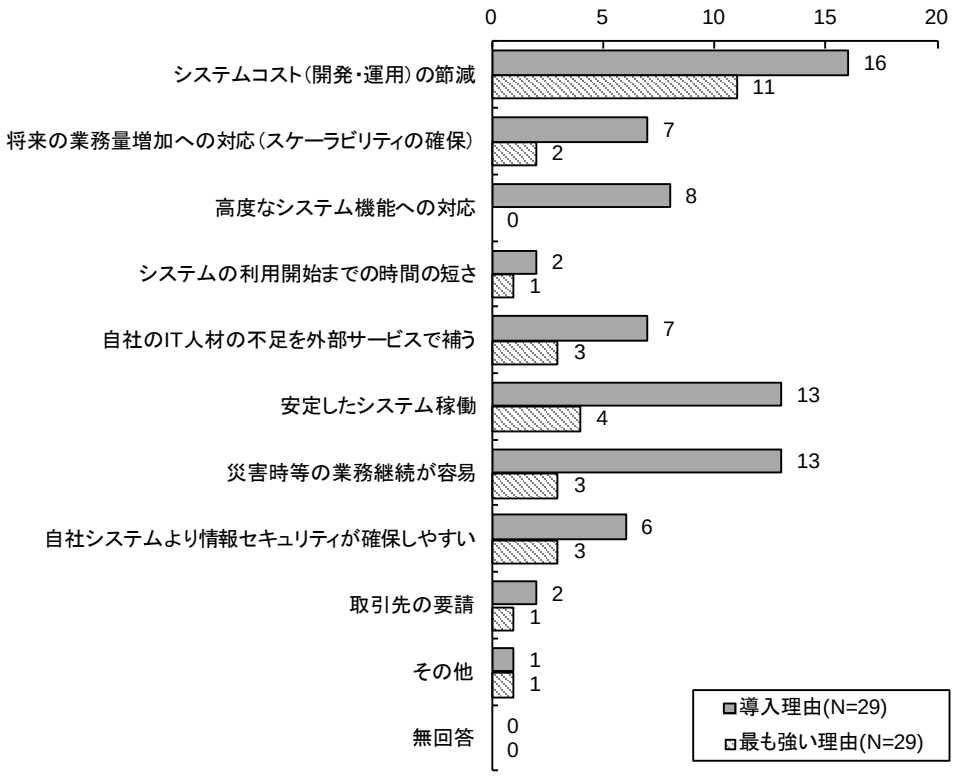
アプリケーション、プラットフォームにおける、アウトソース・外部利用の比率が今回対象とした 8 業務の中で最も低く、自社保有の比率が最も高くなっている。

図表 35 システム利用形態・調達計画（N=45）



クラウドの導入理由も他の業務と同様、「システムコストの節減」、「安定したシステム稼働」、「災害時等の業務継続が容易」の 3 点が多く指摘されており、最も強い理由は「システムコストの節減」である。

図表 36 クラウド導入の理由（調達計画）

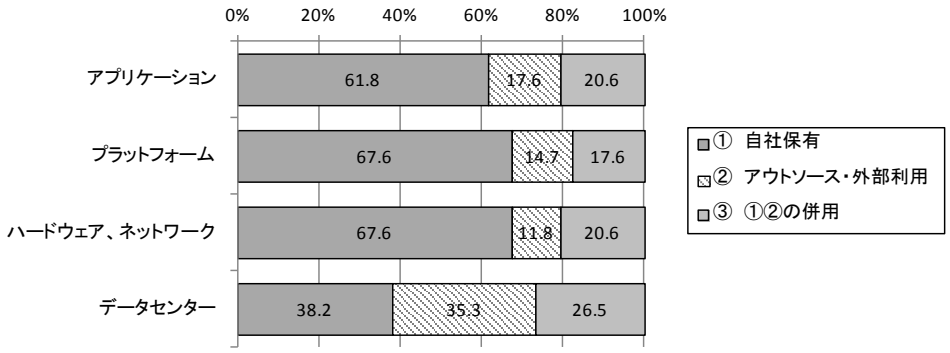


④ 進捗管理

今回対象の 8 業務の中では併用の比率が高くなっている半面、自社保有の比率は低くなっている。

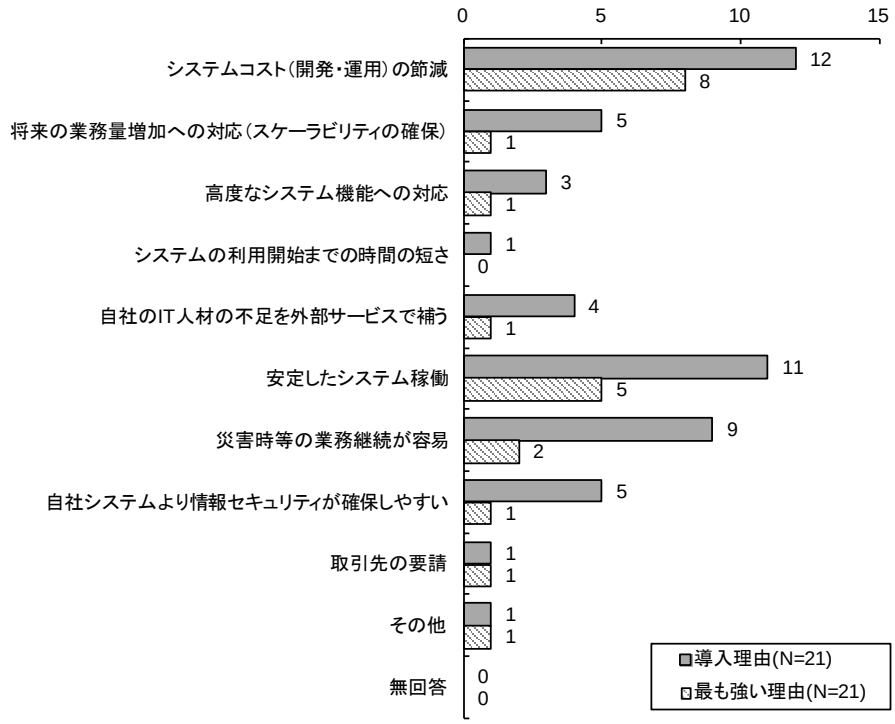
.

図表 37 システム利用形態・進捗管理（N=34）



クラウド導入の理由についても、他の業務の傾向と同様に、「システムコストの節減」、「安定したシステム稼働」、「災害時等の業務継続が容易」という理由が多く、最も強い理由は「システムコストの節減」であった。

図表 38 クラウド導入の理由（進捗管理）

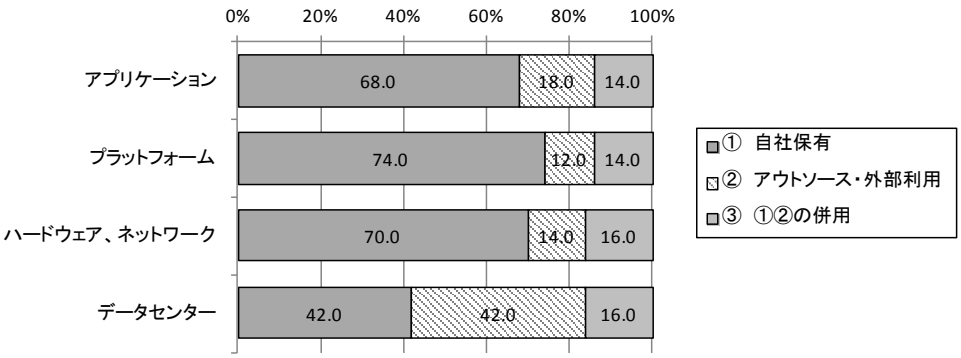


⑤ 調達管理

他の業務と同様、データセンターの外部利用は多いものの、アプリケーション、プラットフォーム、ハードウェア・ネットワークについては自社保有となっている。

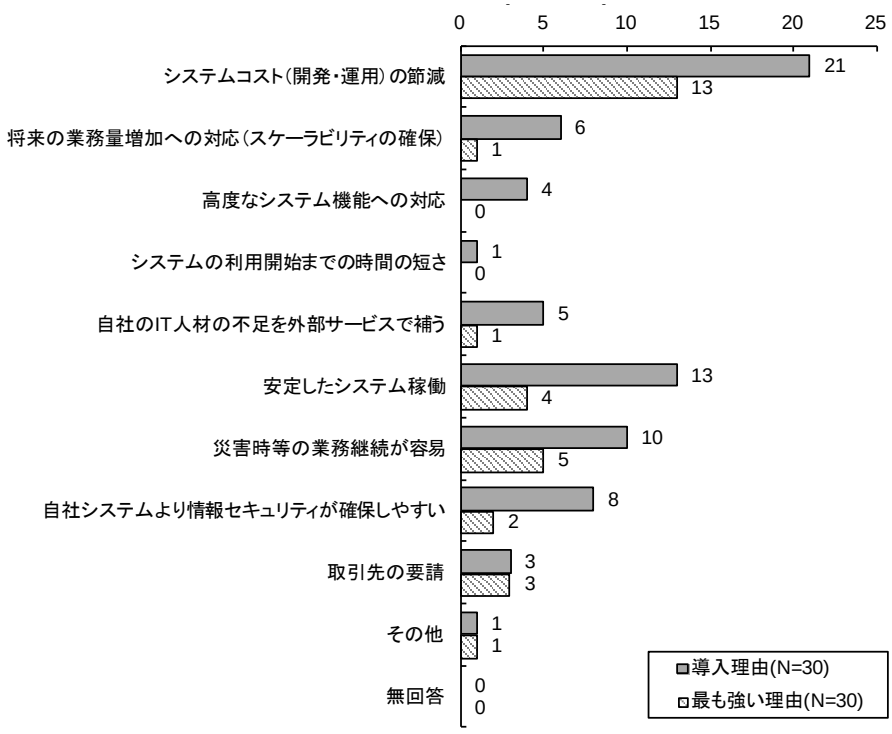
データセンターについては、対象８業務の中でアウトソース・外部利用が最も多かった。

図表 39 システム利用形態・調達管理（N=34）



クラウド導入の理由については、上位３位に「システムコストの節減」、「安定したシステム稼働」、「災害時の業務継続が容易である」、が来ることはは他の業務と変わらない。

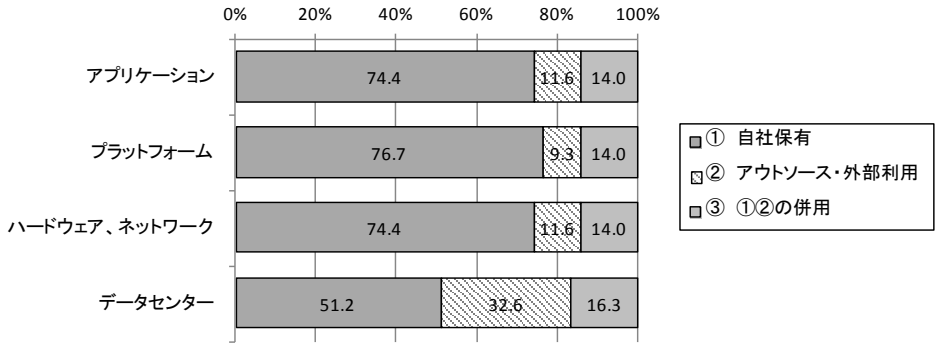
図表 40 クラウド導入の理由（調達管理）



⑥ 生産管理

今回対象とした 8 業務の中ではすべての項目について自社保有の比率が最も高かった。生産管理については、企業や生産ラインごとに独自のノウハウがあるととらえられる傾向にあり、また生産現場で直接使われるものであることから、クラウドの利用が低いと考えられる。

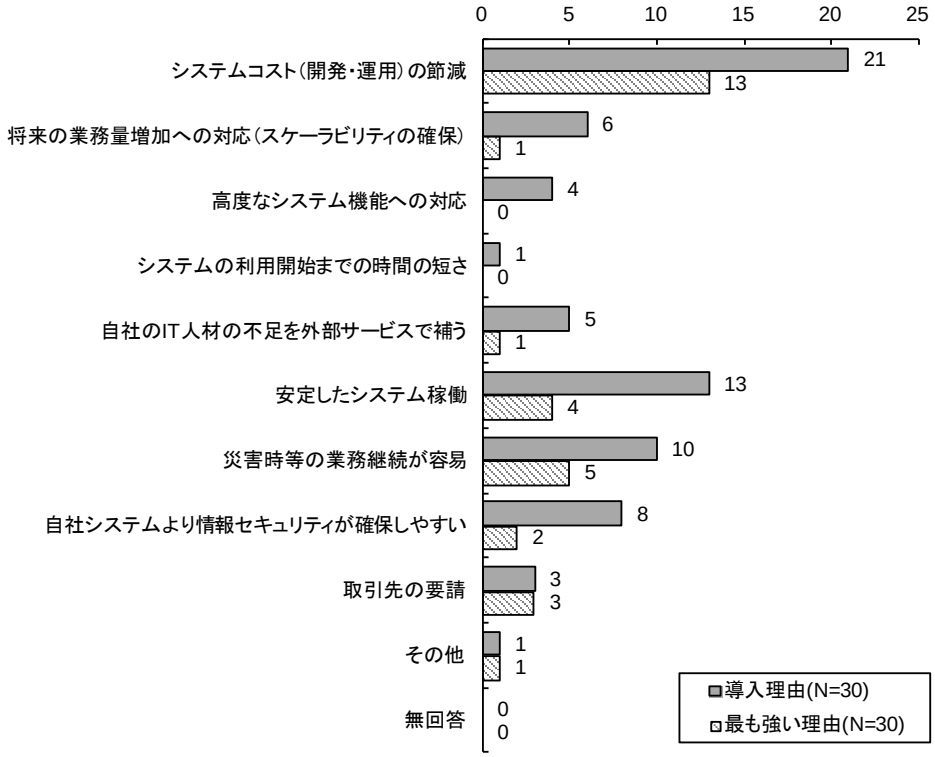
図表 41 システム利用形態・生産管理（N=34）



クラウド導入の理由では、「システムコストの節減」と「災害時等の業務継続」が最も多くなっており、他の業務に比べて災害時等の業務継続に対する期待が高い。

最も強い理由については、他の業務同様である。

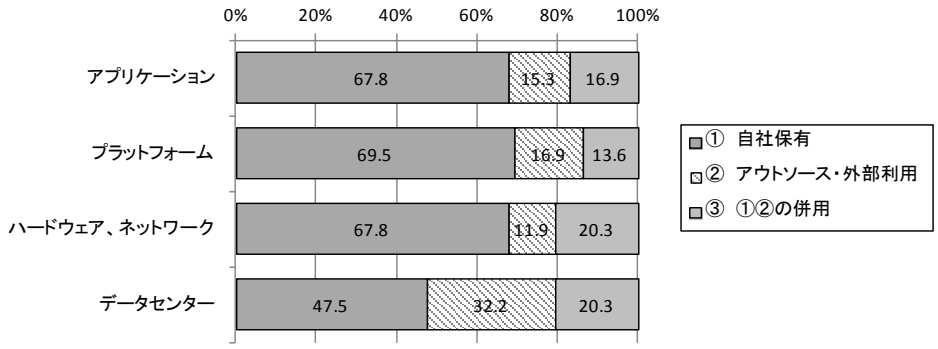
図表 42 クラウド導入の理由（生産管理）



⑦ 販売管理

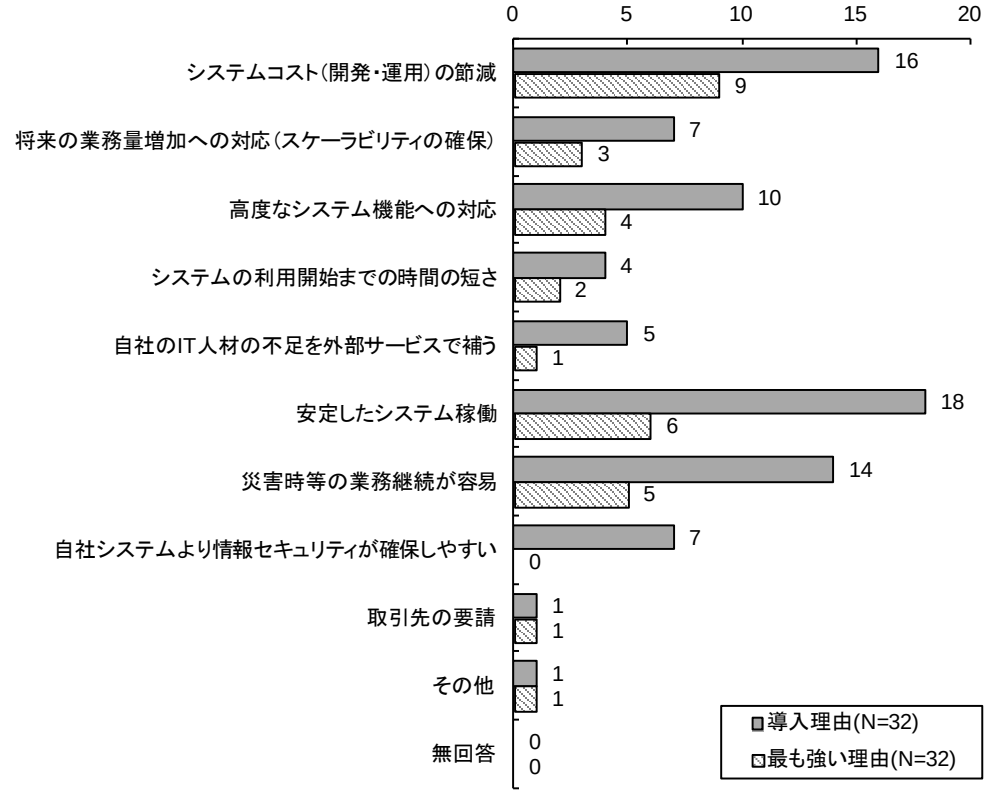
他の業務と同様、データセンターの外部利用は多いものの、アプリケーション、プラットフォーム、ハードウェア・ネットワークについては自社保有が主となっている。

図表 43 システム利用形態・販売管理（N=59）



クラウド導入の理由は「安定したシステム稼働」が最も多く、他の業務とは異なっている。ただし、「システムコストの節減」、「災害時等の業務継続」についても多く指摘されており、上位 3 位は変わらない。最も強い理由は「システムコストの節減」であった。

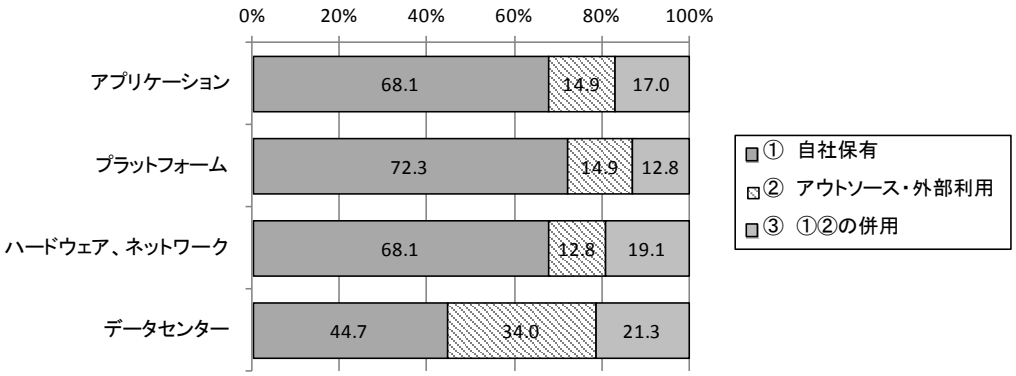
図表 44 クラウド導入の理由（販売管理）



⑧ 財務会計

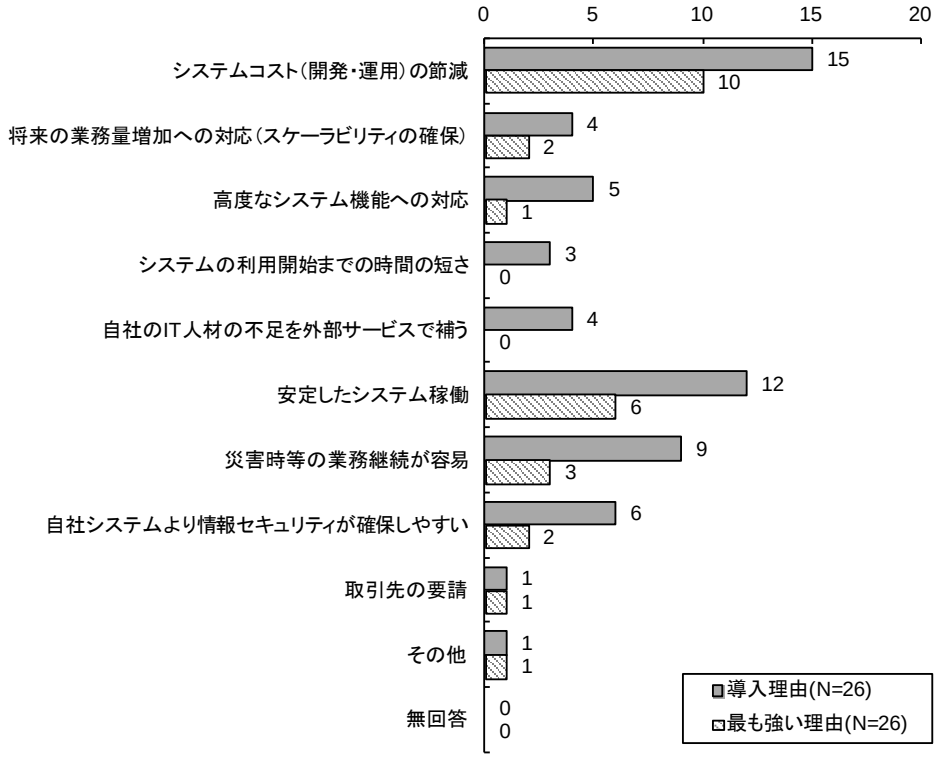
他の業務と同様、データセンターの外部利用は多いものの、アプリケーション、プラットフォーム、ハードウェア・ネットワークについては自社保有が多い。アプリケーションの自社保有比率も 8 業務の中では高い方である。財務会計はパッケージソフトなども豊富でクラウドの利用が進んでいるのではないかと想定していたが、逆に自社保有が多いとの結果となった。

図表 45 システム利用形態・財務会計（N=47）



クラウド導入の理由についても、他の業務と同様に「システムコストの節減」、「安定したシステム稼働」、「災害時の業務継続が容易」というものが多かった。

図表 46 クラウド導入の理由（財務会計）



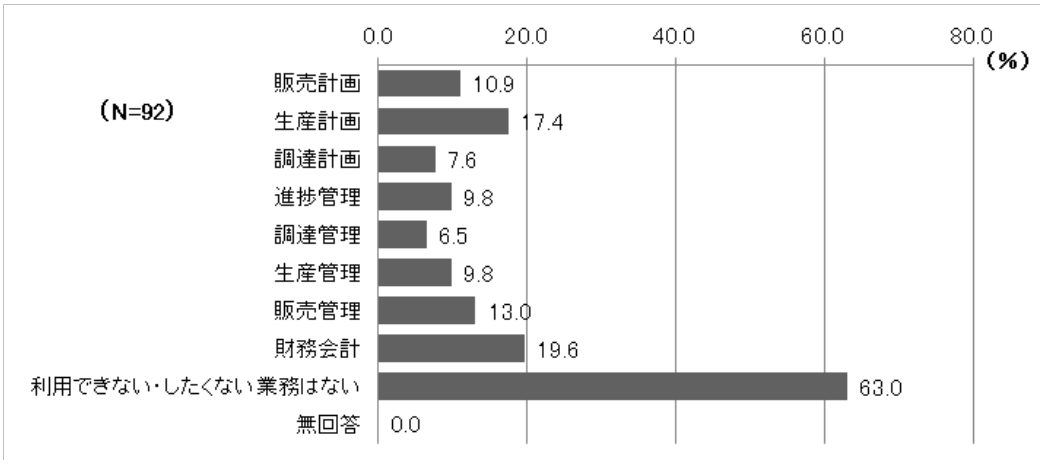
(5) クラウドを利用できない・利用したくない業務

① クラウドを利用できない業務

63%の回答者が「クラウドを利用できない・クラウドを利用したくない業務はない」と回答しており、クラウドを BtoB の情報インフラとして利用することの抵抗感は基本的には少ない。利用できない・したくない業務として指摘が多かったのは以下のものである。

- 財務会計
- 生産計画
- 販売管理

図表 47 クラウドを利用できない・利用したくない業務



② クラウドを利用できない・したくない理由

いずれの業務でも「情報セキュリティに不安があるから」が過半を占めており、特に財務会計では使いたくないとする回答者のうち 94%がその理由として挙げている。「利用できない・したくない」とする回答が多かった業務を見ると、その理由には以下のような特徴がある。

✧ 財務会計

・ 圧倒的に「情報セキュリティへの不安」が挙げられている
・ 次いで、「サービスの安定性」、及び「現行システムで十分だから」

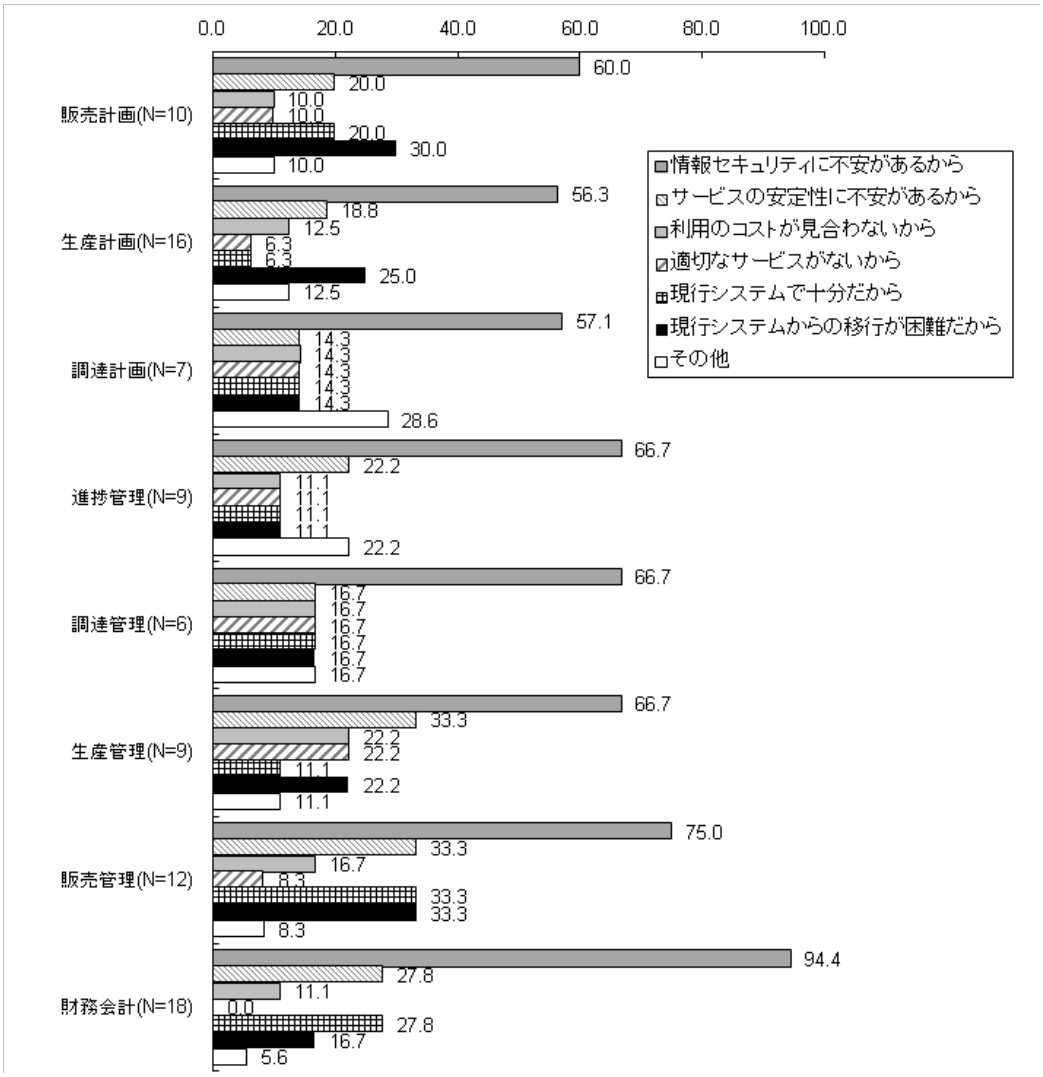
✧ 生産計画

・ 情報セキュリティに続く理由が「現行システムからの移行が困難」である。生産計画策定には独自のノウハウがあるといわれているため、移行が難しいという意見があるものと考えられる。

✧ 販売管理

・ セキュリティ以外の理由は「サービスの安定性」、「現行システムで十分」、「移行の困難さ」が横並びとなっている。

図表 48 クラウドを利用できない・利用したくない理由



(6) クラウドサービスが停止した場合に業務が受ける影響

続いて、クラウドサービスが停止した場合に、業務が受ける影響について、停止期間 1 日および 3 日程度の 2 つのケースに分けて質問した。それぞれ回答は以下のような傾向が見られた。

① 停止期間 1 日程度の影響

「継続困難になる」とするものが多い(40%前後)のは、生産計画及び生産管理である。生産に関わるところは、クラウドサービスの停止による影響が大きい。

「業務の一部に継続できないものが生じる」業務は販売計画と調達管理である。

「すべての業務は継続できるが業務処理の能力が低下する」が多い業務は、進捗管理と販売管理、また調達計画である。

「すべての業務は継続できるが代替手段確保に経済的な負担が生じる」という指摘が多かったのは調達管理、生産管理、販売計画の 3 つである。

一方、「大きな支障なくすべての業務が継続できる」が多かったのは財務会計である。

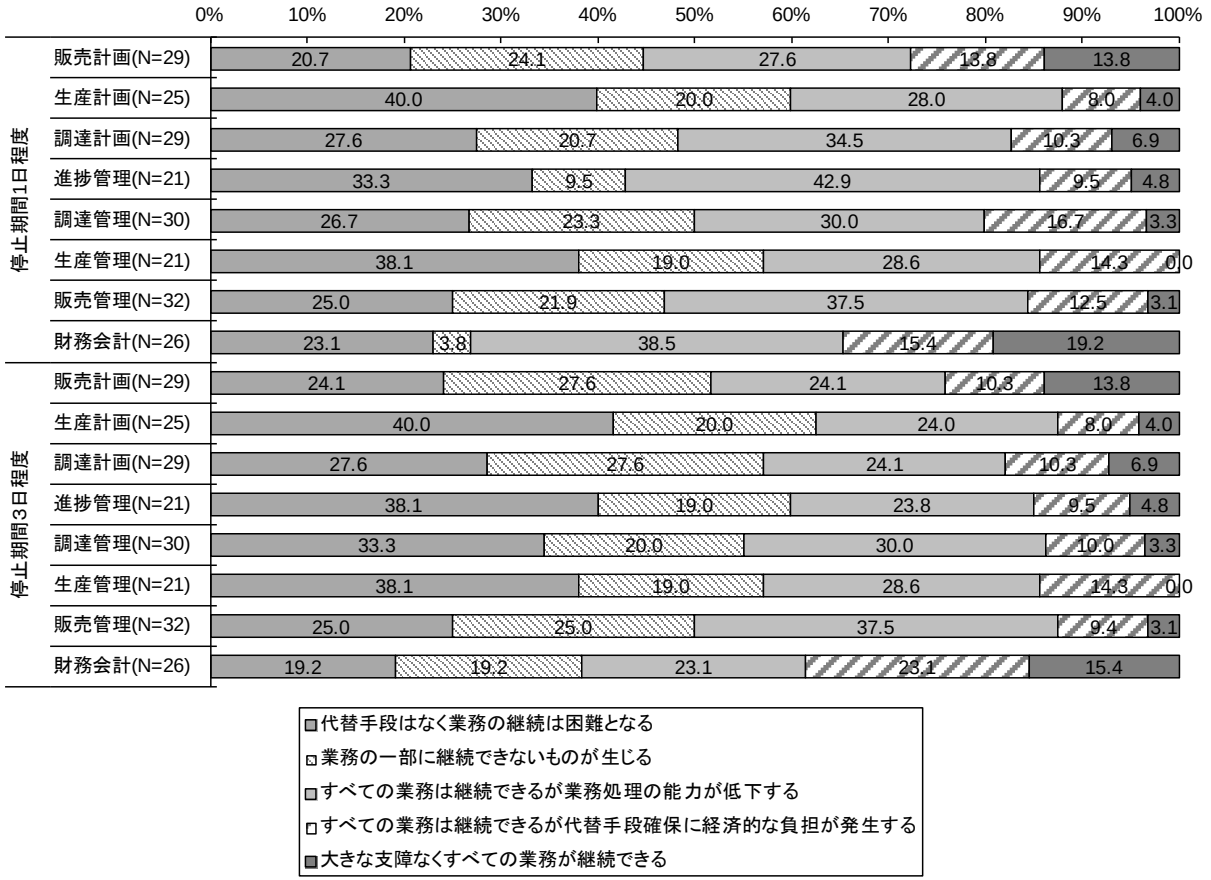
このことから、クラウドが停止した場合に最も影響を受けるのは生産そのものであって、次いで影響が大きいものは販売計画、調達管理となる。

その一方で内部処理が中心の財務会計は影響を受けにくいとの認識である。

② 停止期間 3 日程度の影響

おおむねどの業務でも停止期間 1 日程度の場合の回答と比べて深刻度が増している。全体の傾向は 1 日程度の場合とほぼ同様ではあるが、進捗管理業務や財務会計業務では「業務の一部に継続できないものが生じる」が急増しており、半面「すべての業務は継続できるが業務処理の能力が低下する」という回答が減少している。

図表 49 クラウドサービスが停止した場合の影響

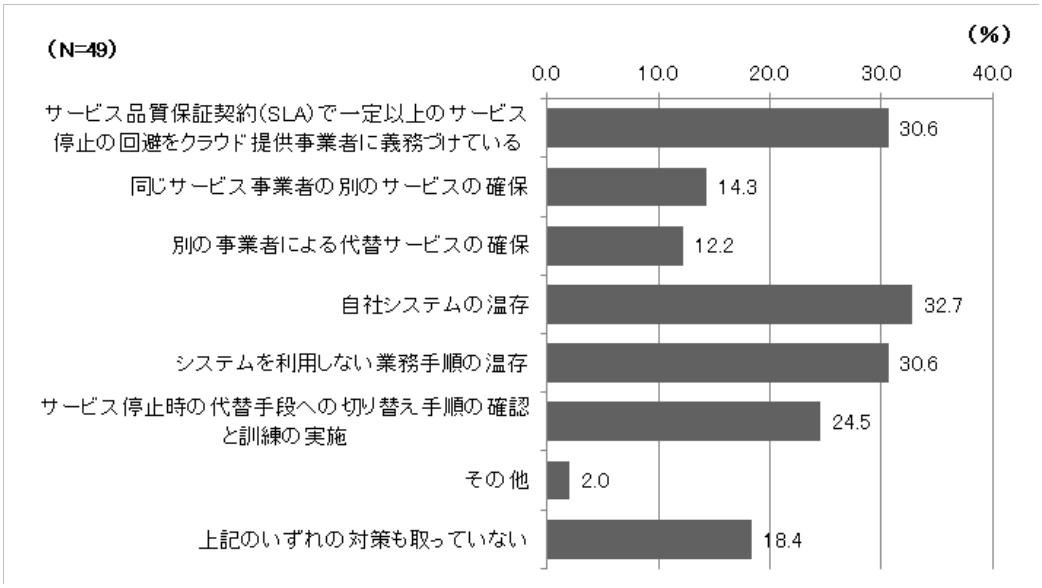


(7) クラウドサービス停止に備えた対策

① 対策の内容

対策で多かったものは「自社システムの温存」、「システムを利用しない業務手順の温存」、「SLA による停止回避を事業者に義務づけ」が多かった。一方、未対応の回答者も 18.4%存在する。

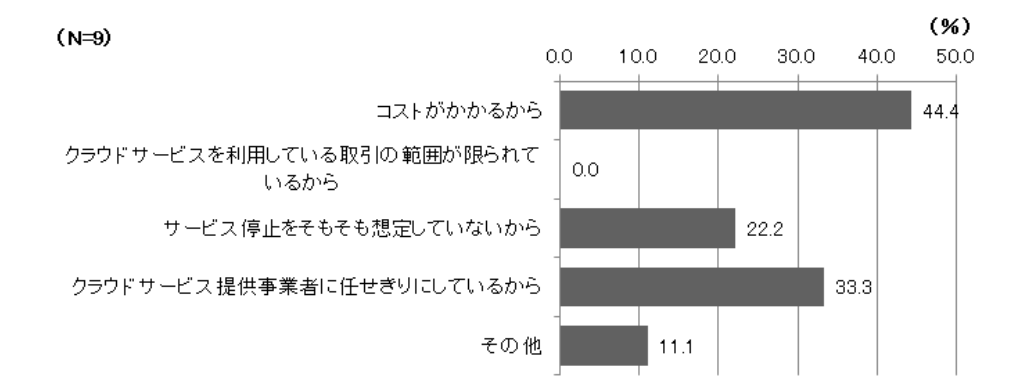
図表 50 クラウドサービス停止に備えた対策



② 未対応の理由

未対応の理由の半数近くはコストが限られていることを挙げており、また、サービス事業者に任せきりにしているからという回答も多い。

図表 51 クラウドサービス停止に備えた対策を取っていない理由

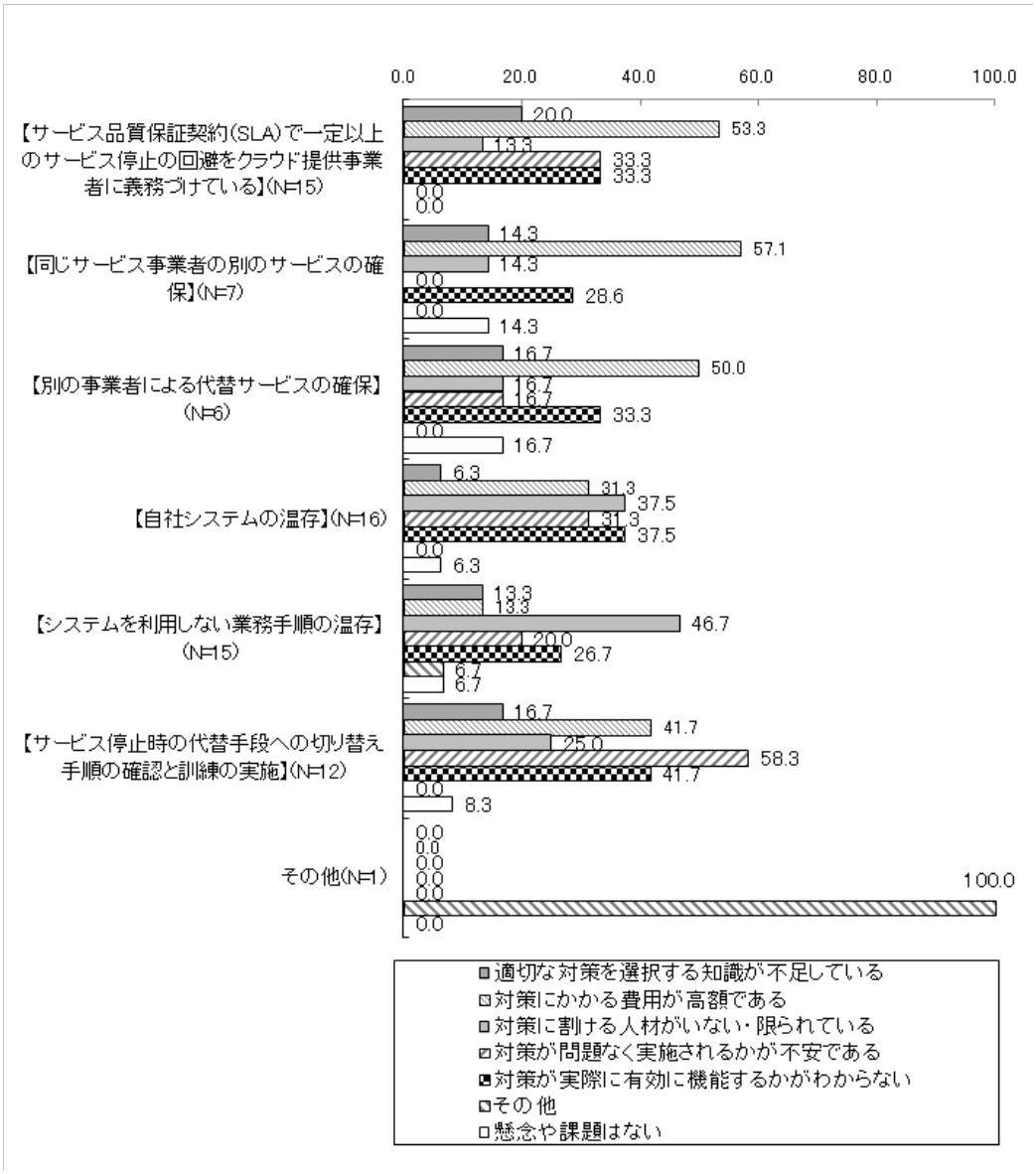


③ 対策に対する懸念

「SLA」「同じ事業者の別サービスの確保」「別の事業者による代替サービス」で

は、対策にかかる費用が高額、対策が実際に有効に機能するかがわからないというものが多い。また、「自社システムの温存」「システムを利用しない業務手順の温存」では対策にかけられる人がいない・限られているという課題が多い。

図表 52 クラウド停止対応策に対する懸念



1.3.3. クラウドの浸透実態と課題

以上のアンケート結果より、企業の生産販売活動や企業間情報連携等において、クラウドは次のように利用されていることが明らかとなった。

クラウドの利用は業務別の傾向には大きな差は見られず、どの業務においても、社外のデータセンターを利用しているものが半数弱と比較的多いものの、それより上位のハードウェア、プラットフォーム、アプリケーションは 60～70%程度が自社保有となっている。すなわち、外部のデータセンターにハウジングを依頼しているものの、それより上位のレイヤーにおけるクラウド利用は 20～30%程度に留まっている。

また、クラウドを利用する動機は構築・運用コストの削減、スケーラビリティの確保、安定運用の実現に加え、災害時対応が多く見られたが、最も強い動機は構築・運用コストの削減であった。ユーザ企業から見て、クラウドは「安く情報システムを利用できるもの」という認識があることがうかがえる。

一方、クラウド化できない業務は 63%が「ない」と答えている一方で、クラウド化ができない業務で比較的多かったものは財務会計、生産計画の 2 業務であった。クラウド化できないとする理由はほとんどがセキュリティへの懸念であり、クラウドの情報セキュリティに対するユーザの疑念が依然として根強いことがうかがえる。

一方、何らかの形でクラウドを利用しているユーザにおけるクラウドの停止時の業務への影響については、クラウドへの依存度によって「業務継続不可」「すべて継続できるが処理能力が低下」の二つに分かれた。停止期間が長いほど深刻度は上がる傾向にはあるが大きな差異は見られなかった。

最後に停止リスクへの対応については、クラウド以外の自社システムや手運用を温存しているという回答が多かった。また、SLA によってクラウド事業者に可用性を担保させている例が多かった。その後のリスク対応への回答結果とも合わせると、クラウド事業者側に一任している傾向もうかがえる。

1.4. 重要インフラ等の情報インフラとしてのクラウド

1.4.1. 調査の概要

内閣官房情報セキュリティセンター（NISC）によって重要インフラに指定されている、情報通信や金融等の 10 分野においてクラウドの導入事例を調査し、クラウドの普及状況とその特徴について把握した。

図表 53 調査対象事例

NISC の分類	クラウドの利用例	概要
情報通信	―	―
金融	• BeSTA （NTT データ）	• 地方銀行の勘定系共同利用型センター。7 行参加、1 行が稼働中。 • これ以外にも NTT データが運営する共同利用型センターがある
	• しんきん共同システム （NTT データ）	• 全国の信用金庫 271 金庫のうち 90%が利用。
航空	• Navitire （アクセンチュア）	• LCC(Low Cost Carrier：低コスト航空会社）向けの BPO、IT アウトソースサービス。業務全般を ASP として提供
鉄道	―	―
電力	―	―
ガス	―	―
政府・ 行政サービス	• 共同アウトソーシング （山形県・置賜広域行政事務組合）	• 3 市 5 町が参加する行政基幹業務の共同利用型システム。 • 12 業務でサービスを利用
	• 奈良県市町村基幹システムクラウド化（奈良県）	• 市町村の基幹業務をクラウド化（共同または単独）
医療	• CIMA Chart SaaS （テクノプロジェクト）	• 電子カルテを SaaS として提供
	• ポケットカルテ （NPO 法人日本・サスティナブル・コミュニティ・センター）	• PHR（Personal Healthcare Record）サービス
	• からだカルテ （株式会社タニタ）	• 体組成計等のデータを元に健康管理を行う PHR サービス（有料会員 20 万名）
水道	• 水神システム （小松電機産業）	• 上下水道施設管理システムの ASP/SaaS。
	• ウォータービジネスクラウド （メタウォーター）	• 上下水道施設管理システムの ASP/SaaS。
物流	―	―

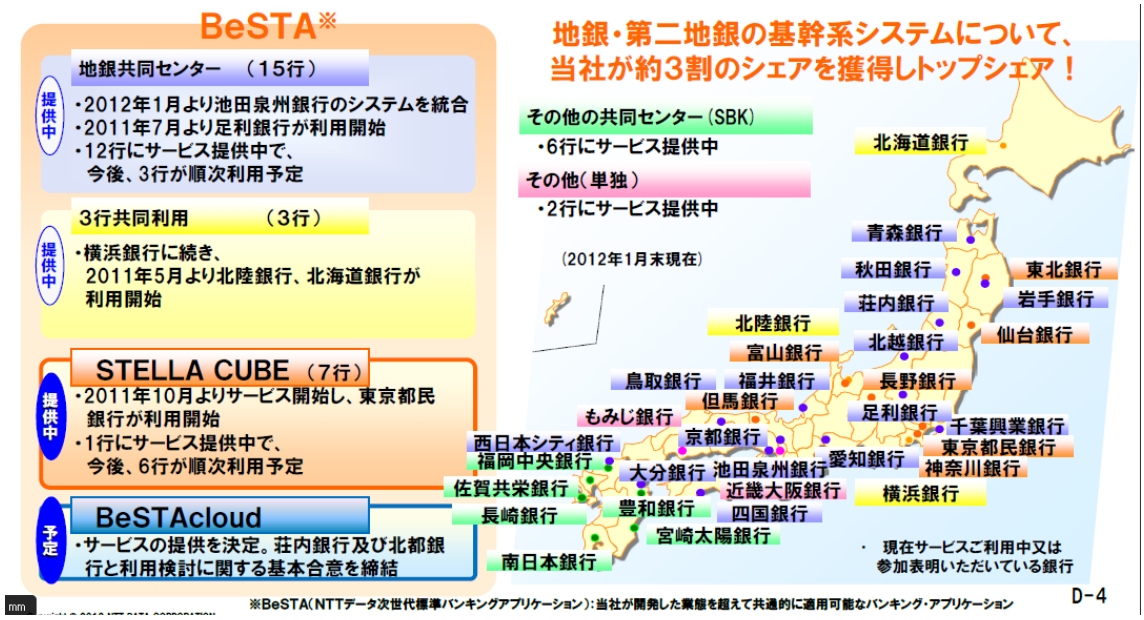
1.4.2. 対象事例

(1) 金融「BeSTA」

NTT データが運用する地方銀行・第二地方銀行向けの基幹系システムの共同利用サービスである。下図に示すように、提供中のサービスは「地銀共同センター」「3 行共同利用」「STELLA CUBE」の 3 つに分かれる。また、「BeSTAclud」サービスを近日提供予定である。これらのサービスを利用している銀行は 2012 年 2 月現在で 25 行、利用開始予定が 11 行である。NTT データによると、地方銀行・第二地銀の基幹系システムの約 30%のシェアを占めているとのことである。

この背景として、地方銀行においては、業務効率化の必要性や経営統合などに伴って、情報システムについても共同利用化を進めていることがある。クラウド型サービスの活用によって、システム投資やコストを少しでも抑えられることが期待されている。

図表 54 BeSTA



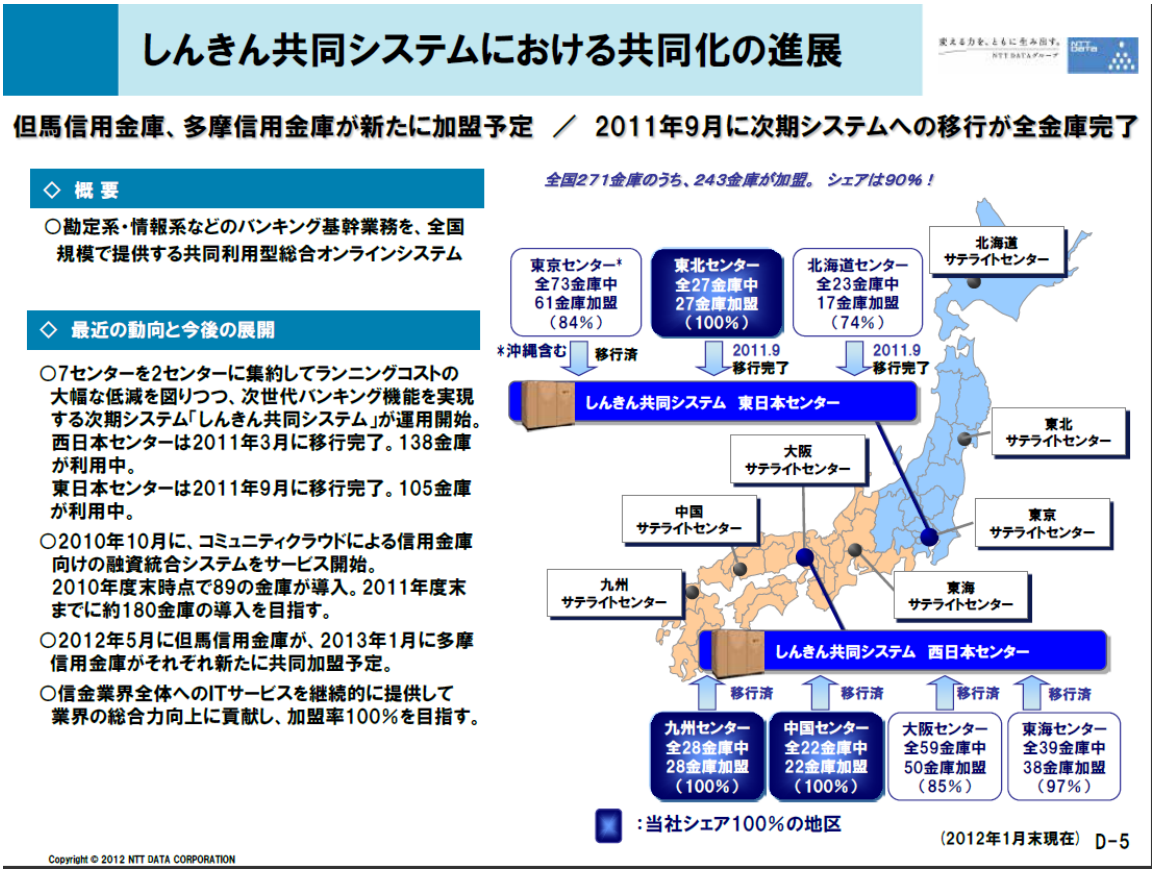
出所）NTT データ IR Information Appendix（2012 年 2～3 月）
http://www.nttdata.com/jp/ja/corporate/ir/library/tool/presentation/pdf/2012/ap1202j_all.pdf
（2012 年 6 月現在）

(2) 金融「しんきん共同システム」

前項と同様に、NTT データが運用する信用金庫向けの勘定系、情報系の基幹業務システムの共同利用サービスである。全国の信用金庫 271 金庫のうち、243 金庫が加盟し、シェアは 90%に達する。

NTT データは 7 センターを東西 2 センターに集約すると同時に次世代システムを稼働させており、コミュニティクラウドサービスを用いた新サービスも運用を開始している。ユーザ側でもシステム運営組織に加え、事務センター機能の統合を図ろうとしており、信用金庫の BPO サービスに発展している。

図表 55 しんきんシステムの概要



出所)NTT データ IR Information Appendix(2012 年 2～3 月)
http://www.nttdata.com/jp/ja/corporate/ir/library/tool/presentation/pdf/2012/ap1202j_all.pdf
(2012 年 6 月現在)

(3) 航空「Navitiare」

アクセンチュアの子会社が提供する航空業務の BPO およびクラウドサービスである。主な機能を下表に記すが、チケット発券、予約管理、顧客ステータス管理などの営業関係の機能に加え、遅延・欠航等の異常運航時における機材・乗員運用の最適化のような基幹業務の機能も有している。

図表 56 Navitiare の主な機能

機能	説明
予約、インターネットおよび直接販売	• Web 直接販売 • 業界標準販売チャネル・バイパス • 大手販売業者への直接アクセス・サービス • ダイナミック一括サービス・パッケージ
売上管理と価格最適化	• RMS[26]（複雑で付帯条件の多い料金体系を維持している航空会社向け） • SkyPrice™（自由な料金体系をとっている航空会社向け）
航空業務と業務リカバリー	• 異常運航時の予想コストおよび航空機、乗員、乗客への影響など、様々なリカバリーの可能性を数分以内で提示 • 日々の乗員、航空機の稼働を最適化 • 乗務時間等の管理により法規制の遵守
バックオフィス	• Revenue Protection はチケット販売の合法性を幅広く監査し、関税法を遵守 • 売上会計：按分や乗継運賃の決済、仕訳記入など • チケットレスな予約環境下での財務管理、財務・売上報告を行うための情報収集

出所）Accenture 日本法人 Web サイト
http://www.accenture.com/jp-ja/outsourcing/bpo/airline/Pages/navitaire-index.aspx（2012 年 6 月現在）から NRI 作成

全世界 85 社以上の航空会社が導入しており、エアアジア等の LCC（Low Cost Career：低コスト航空会社）では約 3 分の 2 のシェアを有する。また、LCC だけではなく、QANTAS オーストラリア航空、エアカナダなどの在来型の大手航空会社にも採用されている。

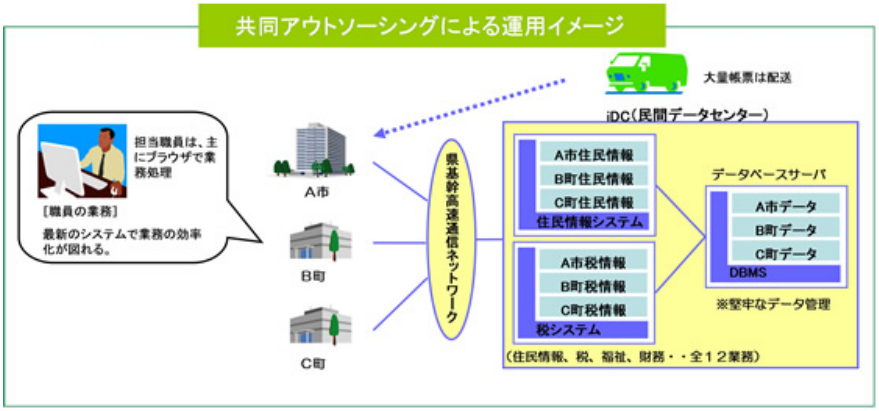
[26] Revenue Management System

（4） 行政「共同アウトソーシング」（山形県・置賜広域行政事務組合）

山形県南部置賜地域の 3 市 5 町の事務組合が運用する基幹業務システムである。基幹業務として提供されているのは下記の 12 種類であるが、参加団体によってシステム更改時期や個別ニーズに合わせて導入機能は異なっている。

①住民情報	②税	③国保年金	④選挙投票
④福祉	⑥介護保険	⑦医療費助成	⑧学齢簿
⑨財務会計	⑩人事給与	⑪上下水道料金	⑫後期高齢者医療

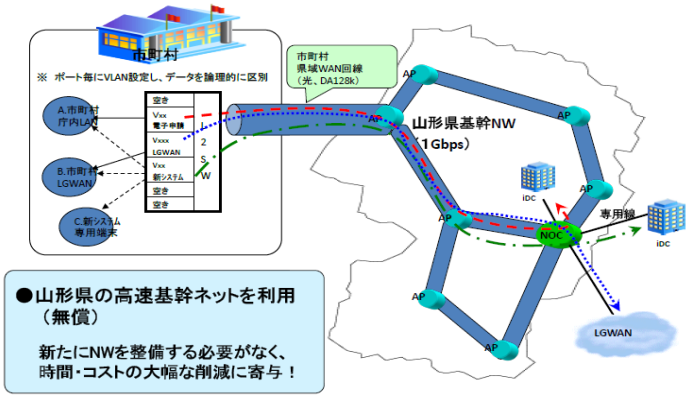
図表 57 共同アウトソーシングの概要



出所）地方自治情報センター「電子自治体ベストプラクティス」
https://www.lasdec.or.jp/its/bestpractice/22saiteki/a04.html（2012 年 6 月現在）

ネットワークは県が整備した基幹ネットワークを活用しており、専用ネットワーク敷設は不要であったため、構築コストの圧縮に役立っている。仙台市内の民間データセンターに共同サーバを設置しており、VLAN を用いてセキュリティを確保している。

図表 58 利用ネットワークの概要



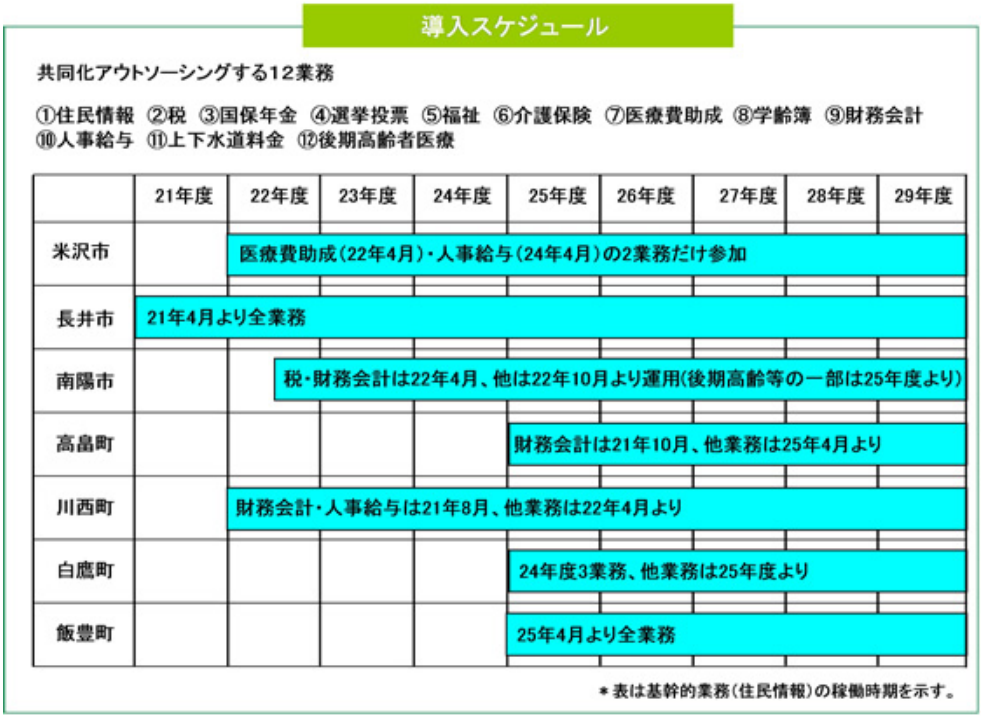
出所）総務省 自治体クラウド推進本部 有識者懇談会（第 4 回）（2011 年 1 月 20 日）資料
http://www.soumu.go.jp/main_content/000099229.pdf（2012 年 6 月現在）

前述したように参加自治体はシステム更改時期に合わせて段階的に導入することができ、コスト削減効果は年間 2 億円程度とみられている。

一方、法律の規定上共同化できない戸籍システムを独自に更新する自治体が出現したことも効果の一つである。すなわち、共同化によってシステムコストが最適化され、節減されたシステム開発費を必要なものへ回せるようになったことの表れと考えられる。

このようにクラウドのスケーラビリティや機能の柔軟性を活かして、システム投資の最適化が実現されている。

図表 59 参加自治体ごとの導入スケジュール



出所）地方自治情報センター「電子自治体ベストプラクティス」
https://www.lasdec.or.jp/its/bestpractice/22saiteki/a04.html（2012 年 6 月現在）

(5) 行政「奈良県市町村基幹システムクラウド化」

奈良県内の市町村においては、任意団体としての「奈良県基幹システム共同化検討会」が共同クラウド化を推進している。地域の事情により一部事務組合ではなく、任意団体として身軽な形態で取り組んでおり、2011 年以降、7 団体が順次 22 業務をクラウド化しているところである。

クラウドを利用するうえでの課題として、停電や通信遮断時において業務が継続できないことがあるが、本システムにおいてはクラウドにデータを預けるだけではなく、各自治体の庁舎内にバックアップサーバを設置している。前日のバックアップデータを取得し、ネットワーク切断時の縮退運用を可能としていることが特徴である。

図表 60 奈良県市町村クラウド化・共同化事業の実施状況

奈良県市町村
クラウド化・共同化事業推進状況

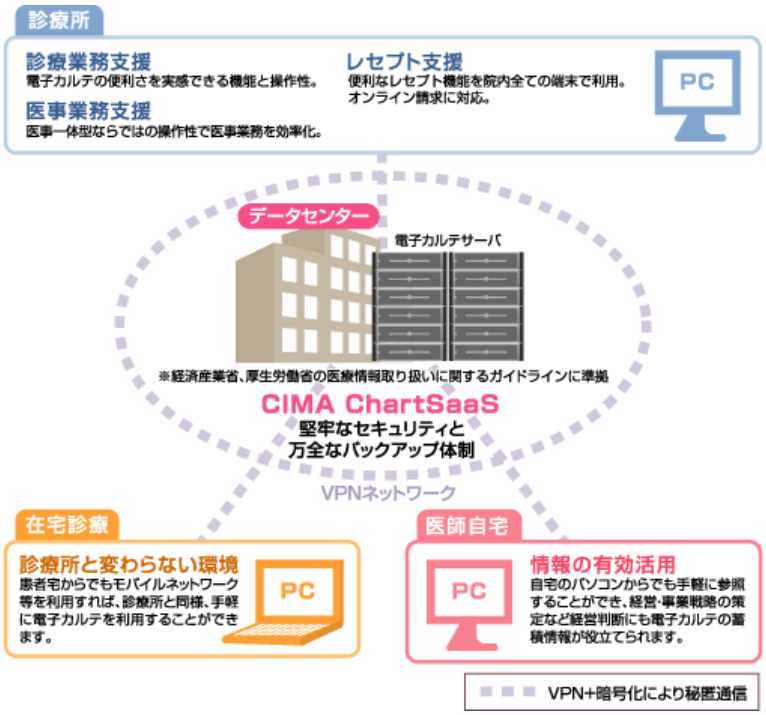
分類	名称		団体数	参加団体名	稼働開始
共同クラウド	奈良県基幹システム共同化検討会（22業務）		7団体	香芝市、葛城市、川西町、田原本町、上牧町、広陵町、河合町	H23.5～順次
単独クラウド			14団体	大和高田市、天理市、宇陀市、平群町、三宅町、曽爾村、御杖村、高取町、明日香村、王寺町、吉野町、下市町、東吉野村、安堵町	H23.1～順次
共同利用	基幹システム共同利用（13業務）		3団体	川上村、上北山村、野迫川村	H23. 4
	財務会計システム共同利用		2団体	河合町、広陵町	H23.10
	人事給与システム共同利用		4団体	河合町、広陵町、安堵町、王寺町	H21. 3
	公有財産管理システム共同利用		3団体	天理市、川西町、田原本町	H20.10
	戸籍システム共同化実施協議会		2団体	御所市、野迫川村	H23. 7
	戸籍事務共同化（吉野広域行政事務組合）		7団体	吉野町、黒滝村、天川村、下北山村、上北山村、川上村、東吉野村	H24. 1～順次
奈良県計	基幹システム	クラウド利用 団体数	21団体	注）単独クラウド＝単一の団体で自治体クラウドサービス(SaaS)を利用する形態	
		共同利用 団体数 (非クラウド)	3団体		
	戸籍システム	共同利用 団体数 (非クラウド)	9団体		

出所）ジャパン・クラウド・シンポジウム（2012 年 3 月 8 日開催）奈良県情報システム課 野田氏講演資料 http://www.japan-cloud.org/consortium/sympo2012/index.html（2012 年 6 月現在）

(6) 医療「CIMA Chart SaaS」

島根県のシステムベンダー㈱テクノプロジェクトが提供する電子カルテの ASP/SaaS である。2012 年 2 月現在、電子カルテの ASP/SaaS に取り組んでいるベンダーは 2 社であり、その 1 社であるテクノプロジェクトのサービスにおいては、電子カルテ（院内、在宅診療用）、検査機器連動機能を提供している。ユーザである医療機関側は、インターネットの VPN でサーバにアクセスし、電子カルテの情報を取得する。

図表 61　SaaS 型電子カルテサービスの例（CIMA Chart SaaS）



出所）㈱テクノプロジェクト　Web ページ
http://product.tpj.co.jp/cima_chart/concept11.html（2012 年 6 月現在）

電子カルテをASP/SaaS で提供する上では信頼性の確保が重要と同社では認識しており、電子カルテを運用するデータセンターやデータセンターからインターネットアクセスポイントまでのバックボーン回線には二重化などの対策を施している。しかしエンドユーザ側には二重化を推奨してはいるものの、コストの関係で二重化が行われるケースは少なく、この部分におけるネットワーク障害にリスクを感じている。

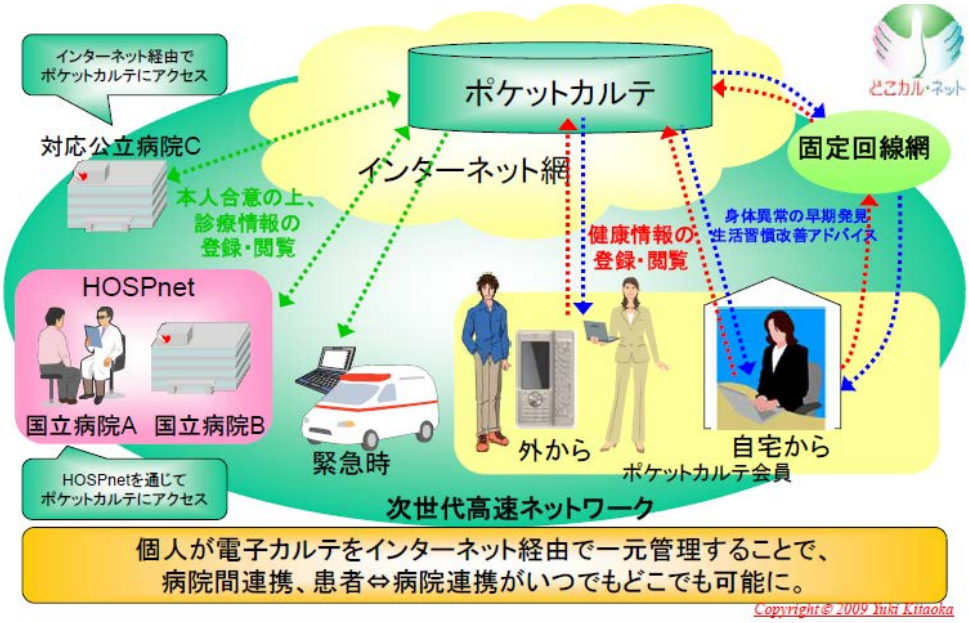
また、アプリケーションの構造に工夫を加え、データの一部をユーザ側にバックアップすることで、縮退運用を行うことを可能としている。さらに在宅医療などでモバイル環境での利用が進んでいるため、通信回線の速度に懸念を持っているという。しかしながら、同社では電子カルテで ASP 化不可能な業務はないと考えている。

(7) 医療「ポケットカルテ」

京都市及び京都府南部の市町において、17 病院、14 クリニックが参加する PHR(Personal Health Record)ネットワークである。運営は特定非営利活動法人(NPO 法人)日本サスティナブル・コミュニティ・センターである。特定健診の結果、投薬記録、医療費などの情報をクラウド上で管理するとともに、患者と医療機関、医療機関同士で情報を共有することにより効果的・効率的な地域医療サービスを提供することを目指している。利用している患者数は 2011 年 2 月時点で約 2 万人である。

- 主な提供機能は以下の通りである。
- 特定健診結果の管理(作成→登録→閲覧)
- 紹介状(診療情報提供書)の管理(作成→登録→閲覧)
- 入退院サマリーの管理(作成→登録→閲覧)
- 電子版お薬手帳
- ヘルスケア家計簿
- 地域共通診察券を利用した医療情報連携

図表 62 ポケットカルテを中心にした医療情報連携の概要



出所)ジャパン・クラウド・シンポジウム(2012 年 3 月 8 日開催)北岡氏講演資料
http://www.kantei.go.jp/jp/singi/it2/iryoujyouhou/dai8/siryou4.pdf(2012 年 6 月現在)

PHR をクラウドで提供する場合には、厚生労働省「医療情報の安全管理に関するガイドライン」をはじめ、SaaS事業者が医療情報を取り扱う際のガイドライン等に準拠する必要があり、本サービスにおいても同ガイドラインに準拠している。また、

個人情報保護については、事業主体は府及び NPO 法人とし、公的な事業として位置づけたほか、データベースを管理するサーバを国立病院機構京都医療センターに設置しており、医療関連情報が民間サイドにおかれないような工夫を行っている。また、地域中核病院であれば災害時等にライフラインが確保されるため、サーバを京都医療センターに設置することは緊急時におけるサービスの継続にも役立っている。

さらに、ネットワーク上の情報セキュリティに関しては、患者サイドで情報閲覧は携帯電話等のネットワークやインターネット VPN を用いており、オープンなネットワークで情報をやりとりしないような工夫を施している。

(8) 医療「からだカルテ」

㈱タニタが提供する PHR サービスである。同社が製造販売する体組成計や歩数計などの計測結果をクラウド上で管理し、PC 等から可視化するサービスである。また、糖尿病管理などでの専門家の指導などのサービスメニューもある。加入者は総数で 20 万人である。

体組成計、歩数計、血圧計での計測データを専用の通信機器、または対応携帯電話でクラウドに送信し、データベースに格納する。

格納したデータを閲覧するいくつかのサービスメニューが用意されており、ハードウェアの利用料とセットで、24 ヶ月契約で月 580 円から 1,800 円までのプランが存在する。通常はこれらのメニューを通じて自己管理のために情報を用いる。専門メニューとして、糖尿病の管理のために専門家の指導付きのコースが用意されており、4 ヶ月 8,400 円の料金を必要とする。

データのアップロードはリレーキーまたはレシーバーと呼ばれる専用機器を用いており、経路上インターネットを利用するがセキュリティ対策は取られているという。閲覧は大手ポータルサイトなどの複数のサービスが対応しており、一定程度の汎用化が図られている。

図表 63 からだカルテを中心にした医療情報連携の概要

出所）株式会社タニタ「からだカルテ」サイト
http://www.karadakarute.jp/info/connect/index.html（2012 年 6 月現在）

（9） 水道「水神システム」

島根県の小松電機産業㈱が提供する、上下水道施設の遠隔監視システムの ASP/SaaS である。全国の 293 自治体 6,000 施設に導入（2012 年 4 月現在）されており、比較的広く普及している。

浄水場、配水場、下水処理施設などの上下水道施設に設置された監視装置が計測したデータを遠隔地で監視するシステムである。通常は専用通信網の整備が必要なところ、インターネットや NTT ドコモの FOMA 網でも利用可能なことから運用コストが低く、全国に広がっている。

集中管理をすることで、一般には施設管理の人員の集約・削減が図れるが、異常を検知した場合に詳細がわからないまま出動するケースがあり、結果的に無駄足になることも多い。しかしこのシステムを用いることにより、緊急時の対応と判断が迅速に行え、効果的な対応と、無駄な対応の削減が図れている。

データの送受信にインターネットを利用することでセキュリティが懸念されるが、制御系ではなく監視系のデータが主であることや、上下水道施設の設備操作は職員がオンサイトで行うことが多いことから、不正アクセスなどの被害は少ないと考えられる。よって、コスト面の優位性を維持するために通常のインターネットを利用している。

図表 64 水神システムの構成

出所）小松電機産業㈱ Web ページ

http://www.komatsuelec.co.jp/komatsuelec/Products/suishin/suishinmainset.html（2012 年 6 月現在）

（10） 水道「ウォータービジネスクラウド」

水環境のエンジニアリング企業、メタウォーター㈱が 2011 年 4 月より提供する上下水道事業者向けのクラウドサービスである。上下水道事業の民間委託の進展や設備老朽化、事業者の技術者の高齢化や退職に伴う技術力の低下に対応することで「持続可能な上下水道事業」を実現することを目的としている。提供されるサービスは以下の通りである。

- 広域監視サービス：広域にわたる上下水道施設の稼動状況や、水位・水質・圧力等の計測値モニタリング
- アセットマネジメントサービス：上下水道の事業者が保有している施設設備の仕様、運転・稼動情報、故障情報、保守情報などの各種情報をデータセンターで一元管理し、資産管理の最適化を図る
- 遠隔支援サービス：専門の技術者がテレビ会議を用いて遠隔地から現場作業員の判断や業務を支援する

2012 年 3 月現在、16 自治体で採用されている。

図表 65 ウォータービジネスクラウドのサービスイメージ

出所）メタウォーター㈱Web サイト
https://www.water-biz-c.com/about/service.html（2012 年 6 月現在）

1.4.3. クラウドの浸透実態と課題

内閣官房情報セキュリティセンター（NISC）に定義された 10 分野の重要インフラにおいて、基幹業務に関わるクラウドまたはシステムの共同利用が分野によっては進んでいることが明らかになった。以下のような分野において顕著に見られる。

- 金融：勘定系の共同利用センターサービスを信用金庫の 90%以上、地方銀行の 30%以上が利用
- 航空：航空会社の運航管理を含む基幹業務システムのクラウドサービスを世界 85 社以上が導入
- 医療：地域医療機関間の PHR ネットワークに 2 万人、民間企業が運営する PHR の有料サービスに 20 万人が加入
- 水道：遠隔監視の SaaS を 293 自治体の 6,000 施設が利用

この他にも、「3　東日本大震災におけるデータセンターの緊急対応の実態と課題（実態調査その3）」 で行ったクラウド事業者インタビューの結果において、大手銀行のセキュリティ・キー・サービス、大手金融業の確定拠出型年金（いわゆる 401k）の Web システム、大手食品メーカーの物流系基幹システム、県庁が中核の病院と連携して構築した救急医療情報システムなど、重要インフラに関連する多くのシステムがクラウドコンピューティングで運用されていることが明らかとなった。

以上のことから、重要インフラの基幹業務を支える情報システムのクラウド利用や共同利用は特定の分野の特定の領域ではかなりの程度進展しているものがああることが明らかとなった。

一方、セキュリティの課題と対応については、以下のようなことが明らかとなった。

まず、データセンターについては、当該分野の法規制やガイドラインに従い、一定以上のセキュリティ対応は取られている。また、PHR システムなどでは非常時におけるライフラインと平常時の情報セキュリティを確保するために、一般のデータセンターではなく地域中核病院にサーバを設置している例も見られる。

ネットワークに関しては、金融や行政などのミッションクリティカルなものについてはプライベートネットワークが利用されており、セキュリティの確保についての責任の所在がはっきりしている。しかし、インターネット VPN や携帯電話網などのオープンな通信回線を用いているサービスも多い。たとえば医療分野における EHR（Electronic Health Record）、PHR など重要性の高い情報を扱うシステムであっても、コスト削減や利用環境の確保のためにオープンな通信回線を利用している例があり、ネットワークの切断によるサービス中断のリスクは認識されている。このことへの対応は大別して以下のような考え方があり、サービスごとに異なる対応を取っている。

第一に、ローカルにバックアップを保有し、縮退運用が可能になっているサービスがある。たとえば、電子カルテの CIMA Chart SaaS や奈良県における自治体システムなどが該当する。

第二に、サービスが中断したり、情報セキュリティが破られたりしても、業務に大きな影響をきたしにくい情報収集系の業務のみをオープンな通信回線で行っているサービスがある。水道分野における水神システムがこれに当たる。

第三に、非常時におけるライフライン途絶によるサービスの中断に対して、災害時における業務実態を検討した上で、センターサーバーに情報を集中させ、あえて縮退運用を前提としていないサービスもある。これは、PHR サービスのポケットカルテなどがそれに該当している。

これらの考え方は、各サービス事業者において、クラウドサービスの特性であるサービス立ち上げの簡便さと構築コストの低廉さと情報セキュリティやサービス継続性のバランスを取った上で選択されているものと考えられる。

2. 東日本大震災におけるクラウドの利活用の実態と課題（実態調査その２）

2.1. 調査の概要

東日本大震災に際して、被災者・被災企業やその救援・支援にあたる行政やボランティア組織に対して、安否確認、情報共有、行政情報発信や被災者支援の情報基盤の用途に、多岐にわたる無償のクラウドサービスが提供された。このことにより、クラウドが緊急時に社会を支える一翼を迅速、広域、かつ効率的に担えるインフラであることが示された。

本節では、東日本大震災に際して活用されたクラウドサービスの具体事例をとりあげて、どの程度役に立ったのかについて定性的に評価するため、支援の提供者、利用者、利用者の IT をサポートする立場の者等へヒアリングを行って検証した。

2.2. 調査の方法

2.2.1. クラウドサービスの事例分析

（独）情報処理推進機構による「東日本大震災に際して提供されたクラウドサービスの事例集」（2011 年 6 月 20 日）に掲載されている事例[27]の中から、典型的な事例を 21 件抽出し、文献調査や聞き取り調査を通じて、サービスの概要、サービスの利用実態、クラウドの有効性を整理した。

抽出に当たっては、同事例集の中で用いられている次の 4 つの用途区分に基づき、偏りのないように、配慮した。

① 情報共有・流通基盤
② 被災者救援活動の情報インフラ
③ 行政情報提供サイトの拡張
④ 被災企業等の緊急情報発信・業務処理

2.2.2. 被災団体の対応実態の分析[28]

被災した地方公共団体における情報システムの復旧・復興に向けた取り組みを整理し、利用者及び利用者の IT をサポートする立場の視点から、クラウド活用の実態を分析した。

2.3. 調査の結果

2.3.1. クラウドサービスの事例分析

分析の対象として抽出したクラウドサービスの事例を図表 66 に示す。

---

27 http://www.ipa.go.jp/about/press/20110620.html

28 本項は、本調査着手前に、野村総合研究所が自主的に実施した調査結果に基づく。

図表 66 分析対象としたクラウドサービスの概要

用途区分	活用事例	クラウド事業者	利用形態 利用目的	利用者
① 情報共有・流通基盤	岩手県の安否情報 Web サイト	日本 IBM	ホスティング	HOPS
	在宅勤務による事業継続	日本 IBM	在宅勤務	立山システム研究所
	被災地医療に生かされた在宅医療クラウド	富士通	在宅医療	祐ホームクリニック
	被災した企業の企業活動、安否確認、情報発信等のためのホスティング	NEC ビッグローブ	ホスティング	情報発信を必要とする組織・団体
	情報提供サイト(sinsai.info)のホスティング	Amazon	負荷分散 代替サイト	OSMJ 及び有志
	携帯メールと位置情報の蓄積・検索・提供「J!ResQ」	日本マイクロソフト	安否情報	日本デジタルオフィス
② 被災者救援活動の情報インフラ	救援情報共有システム「SAHANA」構築	日本 IBM	ホスティング	ひょうごんテック
	輸血用血液製剤の安定供給支援	日本 IBM	ホスティング	日本赤十字社
	被災動物救護支援サービス	富士通	情報共有	宮城県緊急災害時被災動物救援本部
	被災者と NPO をマッチングするクラウドサービス	富士通	支援需給のマッチング	つなプロ
	農山漁村被災者受入れ情報システム	富士通	情報共有・マッチング	農林水産省
	震災復興支援システム	日本マイクロソフト	情報収集・共有	ページワン
③ 行政情報提供サイトの拡張	クラウド環境にミラーサイトを構築し、アクセス集中に対応	日本 IBM	サーバ ミラーリング	浦安市
	「東日本大震災 子どもの学び支援ポータルサイト」にクラウド型情報基盤サービスを提供	日本ユニシス(ユニアデックス)	支援需給のマッチング	各地方公共団体、教育委員会、学校、企業、NPO 等
④ 被災企業等の緊急情報発信・業務処理	アクセス急増した震災情報システムに IaaS 環境で迅速に対応	富士通	ホスティング	ESRI japan
	被災地向け安否確認・Web 会議の提供	富士通	Web 会議 SaaS	自治体、企業、非営利団体等
	大学連携高度教育基盤システム	ニフティ(CA Technologies)	教材の 相互活用	大学 e ラーニング協議会/各大学
	取引先企業の被災状況や工場稼働状況の確認	日本ユニシス	情報収集・共有	震災や停電の影響で資材や部品調達が難航し、取引先の状況確認が必要な企業や団体
	サーバ、PC の重要データを保存し共有できる場所を提供	日立システムズ	データ保管・共有	自治体、企業等

用途区分	活用事例	クラウド事業者	利用形態 利用目的	利用者
	仮想デスクトップ提供	日立システムズ	情報保存・共有	自治体、企業等
	仮想サーバのリソースを無償で提供	ソフトバンクテレコム	ホスティング	助けあいジャパン

各事例における利用実態やその効果についての詳細を以下に示す。

① 情報共有・流通基盤

活用事例： 岩手県の安否情報 Web サイト

クラウド事業者	日本 IBM(株)
サービス名／サービス種類	IBM Smart Business Cloud
有償／無償	無償
利用者	(株)HOPS
利用形態・利用目的	ホスティング
利用内容	被災者情報共有の情報サイト構築
期間（開始時期）	2011 年 3 月 15 日　から開始

■ サービスの概要

岩手県の安否情報 Web サイトを、IBM Smart Business Cloud 上に構築し、早期に県内被災者の安否情報を提供した。

- 岩手県の若者達で成り立つ NPO から Web サイト立ち上げの話が持ち上がり、Web サイト制作会社である HOPS が構築した。
- 岩手県内限定の情報開示用にクラウドのインフラを探していた HOPS が、IBM の無償提供プログラムをニュースで知り、3/14 午前 0 時過ぎメールで申請。翌 9 時 15 分頃、双方担当者が直接電話で会話。日本 IBM は案件の緊急性を考慮し、数分でクラウドのインスタンスを提供。
- 結果として、岩手県の被災者の安否情報は IBM Smart Business Cloud 上でどこよりも早く発信された。

■ サービスの利用実態

(株)HOPS代表取締役社長によるコメント[29]

> 今回の経験から、パブリッククラウドにはホスティングサービスにはない「手軽さ」があると感じました。今回日本IBMを選んだ理由は「手軽さ」を意識したところにあります。「手軽さ」と「スピード」はクラウドの大きな役割であると感じます。

■ クラウドの有効性

日本IBM(株)によるコメント[30]

> 岩手県の被災者の安否情報をどこよりも早く発信。迅速な安否情報を提供が多くの被災者の方々に安堵感を与えることができた。

・ インターネットを経由して、リモートのデータセンター上にわずか数分で仮想サーバを立ち上げることができたこと、サービスを提供するデータセンターが海外であったため、地震の影響を全く受けることがなかったこと、によって迅速性、耐災性の面で、クラウドの有効性が発揮された。

活用事例： 在宅勤務による事業を継続

クラウド事業者	日本 IBM(株)
サービス名／サービス種類	LotusLive
有償／無償	有償（震災以前に導入済みの企業の事例）
利用者	(株)立山システム研究所
利用形態・利用目的	在宅勤務
利用内容	在宅勤務による事業継続
期間（開始時期）	2011 年 1 月から導入

■ サービスの概要

LotusLive は、社内外の情報共有を円滑に進めるコミュニケーション基盤をクラウド型で提供するサービス。場所を問わず働ける環境を実現でき、東日本大震災後も社外の関係者を含めて早期に業務を復旧し事業を継続可能とした。

・ 「メール/カレンダー＆スケジュール機能」、「コラボレーション・スペース機能」、「Web 会議

[29] http://www-06.ibm.com/ibm/jp/provision/no70/pdf/70_interview3.pdf （2012 年 3 月現在）

[30] 日本 IBM への照会結果による。

機能」の 3 種類のサービスから構成され、必要な機能を単体で利用することも、統合的に組み合わせて利用することも可能。

・ また、社内にかぎらずインターネットに接続可能な環境があれば場所を問わず利用でき、取引先に対しても無償のゲスト・アカウントを発行できるため、不測の事態に備えて取引先も含めた事業継続性を確保する上でも有効。

図表 67 LotusLive におけるゲスト・アカウントの考え方

出所）http://www-06.ibm.com/software/jp/cloud/casestudies/tateyama.html（2012 年 7 月確認）

■ サービスの利用実態

(株)立山システム研究所　東京営業所セクションマネージャーによるコメント [31]

・ 「自宅から3G回線でLotusLiveにアクセスして、必要な資料を参照・更新したり、パートナーとコミュニケーションを取ることができたので、在宅勤務期間も普段、会社で仕事をしている時とさほど変わらずスムーズに業務を遂行することができました。」

・ 「実は震災当日、ちょうど LotusLive のアクティビティー上でやり取りしていた取引先のご担当者が帰社も帰宅も困難になり、ある案件を完全にストップせざるを得ない状況でした。その際、最寄の公共施設に一時避難されたそうなのですが、そこからノートPCでLotusLiveにアクセスしてアクティビティーに参加して下さったので、ごく短期間で業務を復旧することができました。」

■ クラウドの有効性

・ 発災後も、通常のように、場所を問わずに柔軟に働ける環境が提供されており、耐災性の面においてクラウドの有効性が発揮された。

31 http://www-06.ibm.com/software/jp/cloud/casestudies/tateyama.html（2012 年 3 月現在）

活用事例： 被災地医療に生かされた在宅医療クラウド

クラウド事業者	富士通(株)
サービス名／サービス種類	在宅医療クラウド
有償／無償	無償
利用者	祐ホームクリニック （医療法人社団 鉄祐会）
利用形態・利用目的	在宅医療
利用内容	東日本大震災で被災した高齢者の在宅医療をクラウドで提供
期間（開始時期）	2011 年 9 月 3 日から分院開設

■ サービスの概要 [32]

祐ホームクリニック（東京都文京区）は、「被災地で十分な医療サービスを受けられない高齢者への対応や心のケアが、これまで以上に必要になる」と考え、2011 年 9 月 3 日、特に甚大な被害を受けた地域の一つである宮城県石巻市に分院「祐ホームクリニック石巻」を開所。医療のサービスと、それを核とした高齢者の生活を支えるコミュニティづくりに向け活動を始めた。

祐ホームクリニックの取り組みに賛同した富士通は、生活/健康情報などの管理をクラウド上で行うシステムを提供し、取り組みを ICT 分野から全面的に支援。在宅医療時の課題であった、医師や看護師、介護士間での情報共有を ICT で行う支援から開始し、現在は生活/健康情報や訪問スケジュールなどの管理をすべて行う「在宅医療クラウド」を構築している。

＜背景＞

東日本大震災では、多くの医療機関も甚大な被害を受けた。その後、診療を再開する医療機関も徐々に現れてはいるが、まだ十分な医療サービスを提供できていないのが実情である。

復旧の目途が全く立たない医療機関に通院していた高齢者の方も多く、避難所や仮設住宅から遠く離れた都市部の医療機関に通院するのは、容易なことではない。

■ サービスの利用実態 [33]

医療機関の被災等により、被災地で十分な医療サービスを受けられない高齢者を支援する在宅医療において、医師と看護師、介護士等での情報共有や、訪問診療の支援等をクラウドサービスによって提供し、非常に役に立った。

---

[32] http://jp.fujitsu.com/about/csr/recovery/episode3/（2012 年 3 月現在）

[33] 富士通への照会結果による。

■ クラウドの有効性 [34]

迅速性（短期間で構築、サービス開始が可能）、拡張性（利用実態に合わせて能力を拡張することが可能）の面でクラウドの有効性が確認された。

活用事例： 被災した企業の企業活動、安否確認、情報発信等のためのホスティング

クラウド事業者	NEC ビッグローブ(株)
サービス名／サービス種類	BIGLOBE クラウドホスティング
有償／無償	無償
利用者	被災者、復興支援のため情報発信を必要とする組織・団体
利用形態・利用目的	ホスティング
利用内容	被災した企業の企業活動に必要なシステム利用のためのサービス基盤や、安否確認情報、交通情報、鉄道の運行状況など被災地に必要な情報の情報発信
期間（開始時期）	2011 年 3 月～12 月

■ サービスの概要

- 仮想サーバによってリソースをオンデマンドで利用できるクラウドサービス（IaaS）。
- サーバ仮想化技術には、VMware 社の「VMWare」を利用。
- 東日本大震災に際し、被災した企業における通常の企業活動に必要なシステム利用のためのサービス基盤として、また安否確認情報、交通情報、鉄道の運行状況など被災地に必要な情報を迅速に届けるための情報発信を行う組織・団体向けに、「BIGLOBEクラウドホスティング」の無償IDが提供された [35]。

■ サービスの利用実態 [36]

- 東北地方の大学の緊急用 Web サイト： 東北地方の大学において、大学 Web サイト用サーバの機能停止による緊急対応として「BIGLOBE クラウドホスティング」上に大学 Web サイトを立ち上げ、大学関係者の安否確認や、卒業式や、入学式の連絡用に活用。
- 都内の水道水に含まれている放射能調査： 都内の浄水場が公表している水道水に含まれている放射能の量をグラフ化して、浄水場ごとにまとめたサイトを公開。

34 富士通への照会結果による。

35 http://www.biglobe.co.jp/pressroom/2011/03/17-3（2012 年 6 月現在）

36 NEC ビッグローブへの照会結果による。

図表 68 BIGLOBE クラウドホスティングの概要

出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■ クラウドの有効性

短期間で、クラウドホスティングの無償 ID を発行してサービスを提供しており、迅速性の面でクラウドの有効性が発揮された。

活用事例： 情報提供サイトのホスティング

クラウド事業者	Amazon Data Services Japan(株)
サービス名／サービス種類	Amazon Web Service
有償／無償	無償
利用者	一般社団法人オープンストリートマップ・ファウンデーション・ジャパン(OSMFJ)および有志
利用形態・利用目的	負荷分散、代替サイト
利用内容	情報提供サイトのホスティング 情報提供サイトの開発環境の提供
期間（開始時期）	2011 年 3 月～6 月

■ サービスの概要

発災後、安否確認や救護や物資の要請などの情報を位置情報とひもづけて地図上で共有することのできる Web サイト：sinsai.info を、一般社団法人オープンストリートマップ・ファウンデーション・ジャパン(OSMFJ)及び有志が、立ちあげた。sinsai.info は多数の利用者がアクセスしたため、リソースが逼迫した。このため、Amazon Web Service による代替サーバでホスティングを行った。sinsai.info はサービスを安定的に提供でき、多くのユーザに利用された。

また、このプロジェクトはオープンソースの仲間のボランタリーな参加による共同作業を行うことで、短期間にサービスを立ち上げるとともに、長期間、データの吸い上げや翻訳作業といった地味な作業を継続的に実施している。この共同作業にも、AWS から提供された開発環境が役立てられ、遠隔からの参加や各自の空き時間を利用しての参加を可能にし、効率、協働、遠隔参加、持続といったクラウドならではの効果を享受できている。

■ サービスの利用実態

sinsai.info開発責任者のコメント [37]

- 震災翌日というタイミングで、こちらのリソースも非常に圧迫されている中、インフラを無償で提供いただき、またインフラ構築をサポートいただいた方々の存在はとても頼りになりました。
- おそらくあのサポートがなければ sinsai.info はもっと小さなスケールのサービスになっていたと思われます。

■ クラウドの有効性

知識さえあればすぐに利用可能なサーバが何台でも作成できた、利用状況に合わせ柔軟に使われたことから、迅速性、拡張性の面でクラウドの有効性が発揮された。

また、全てホスティングするよりは安かった、あの災害時でも使えていた、ホストが各地に分散できるという点から、経済性、耐災性の面でも評価できる。

図表 69 sinsai.info の画面（2011 年 5 月 24 日頃）

http://www.sinsai.info/

[37] sinsai.info 開発責任者への照会結果による。

活用事例：　携帯メールと位置情報の蓄積・検索・提供「J!ResQ」

クラウド事業者	日本マイクロソフト(株)
サービス名／サービス種類	Microsoft Windows Azure Platform
有償／無償	無償
利用者	日本デジタルオフィス(株)
利用形態・利用目的	安否情報
利用内容	被災時の緊急連絡に、ボイス対応被災時緊急連絡用アプリ「J!ResQ」を無償提供
期間（開始時期）	2011/3/18　からシステム提供

■　サービスの概要

携帯電話およびスマートフォン向けの被災時緊急連絡用アプリ「J!ResQ」を開発し、無償提供を行った。

被災者の方が、携帯電話やスマートフォンを利用して、自分の位置情報と音声を、あらかじめ登録したメールアドレスに自動送信できる。これにより、自分の無事をご家族やご友人に容易に知らせることができる。

J!ResQ で被災者が送信した位置情報と音声のデータは、日本マイクロソフトのクラウドプラットフォームである Microsoft Windows Azure Platform に自動的に蓄積されるため、J!ResQ のメール送信先に入っていない方でも、発信者のメールアドレスで検索することで知人の消息を確認できる。

図表 70 J!ResQ の概要

出所）http://www.do-cat.com/kinou_jresq/index.htm（2012 年 7 月 31 日）

クラウドを利用することで、各種スマートフォンや携帯電話に対応したアプリの迅速な開発・提供や、今後の多言語対応による世界各国での利用が可能となった。

■ サービスの利用実態

日本デジタルオフィス代表取締役社長のコメント[38]

- 震災から 3 日でアプリを完成させることができました。マイクロソフト様のご協力により、震災翌日から無料のクラウド環境で開発できたことが非常にありがたく、従来のオンプレミスでは不可能であったと考えています。
- 今回のアプリではデータベースも利用しているのでその構築にも手間がかからず、早期構築を実現できました。

J!ResQ のダウンロード数は累計 78,000（iPhone、Android の合計）で、継続利用ユーザ数は約 1,700 人。

■ クラウドの有効性

発災後数日でサービスを提供できたことから迅速性の面でクラウドの有効性が発揮された。

海外に立地するデータセンターであることによる耐災性、アクセスが集中してもリソースを拡張できる拡張性も評価できる。

② 被災者救援活動の情報インフラ

活用事例： 救援情報共有システム「SAHANA」構築

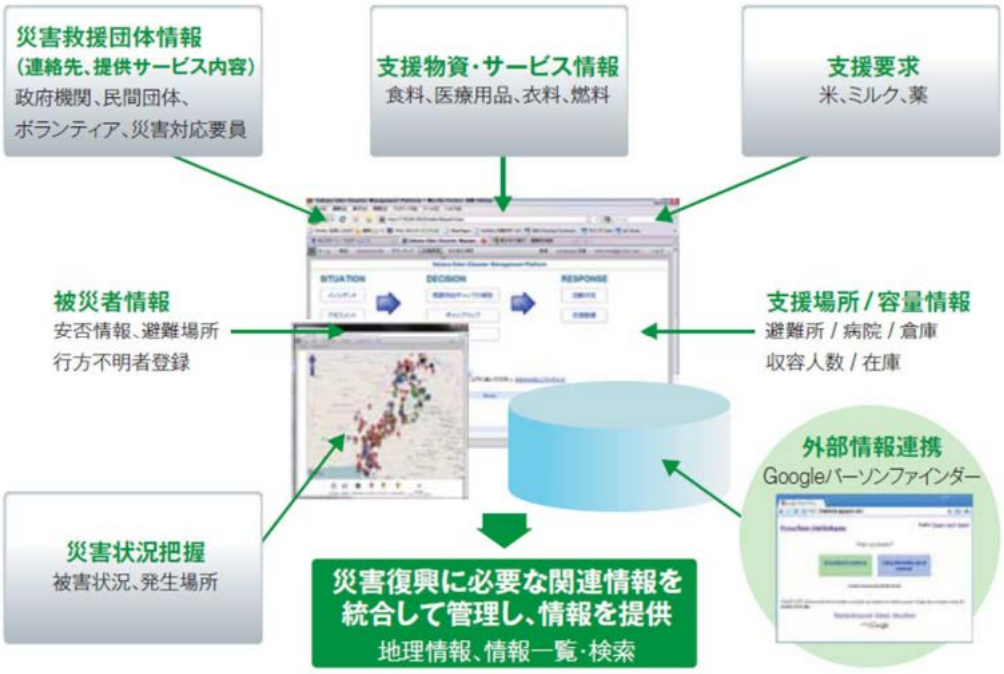
クラウド事業者	日本 IBM(株)
サービス名／サービス種類	IBM Smart Business Cloud
有償／無償	無償
利用者	ひょうごんテック （ひょうご NPO 情報通信技術支援ネットワーク）
利用形態・利用目的	ホスティング
利用内容	災害時の救援情報共有パッケージ・ツール SAHANA を IBM Cloud 上に構築
期間（開始時期）	2011/3/17 クラウド利用開始、5/31Sahana 公開

[38] 日本デジタルオフィスへの照会結果による。

■ サービスの概要

救援情報共有システム「SAHANA」を IBM Cloud 上に構築。東日本大震災において、岩手県と山形県に採用された。

図表 71 救援情報共有システム（SAHANA）の概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

＜SAHANA について＞

- 2004 年に発生したスマトラ島沖地震の際に、スリランカのボランティアによって開発されたオープンソースソフトウェア。
- その後も各被災地における救援情報の共有で成果をあげていたが、関係者が独自にサーバを構築して活用する仕組みだった。

■ サービスの利用実態

ひょうごんテックによるコメント [39]

> 今回の経験を通じて、危機的状況でスピードを求められるときに、すぐ立ちあげられ自由に設定できるクラウドは、危機管理・事業継続において最適の形態だと強く感じました。特にシステムが必要だがあまり投資できないという企業にとって、クラウドは相性がいいのではないでしょうか。

[39] http://www-06.ibm.com/ibm/jp/provision/no70/pdf/70_interview3.pdf（2012 年 3 月現在）

SAHANAに関する報道記事 [40]

- 岩手県では、5 月末から陸前高田市の全避難所を対象に、避難者人数、通所避難者の人数、災害弱者の方の人数、各避難所のライフライン復旧情報の把握といった、被災状況や被災者の情報を一元的に管理。さらに、それぞれの避難所から、NTT ドコモが設置したタブレット端末「GALAXY Tab」を利用して、必要物資の要望を把握できるようにした。
- 山形県では、SAHANA を活用することで、福島県からの避難者の所在情報を一元管理したという。山形県は避難者に対して、当初の一次避難所からホテルやアパートへの二次避難を推進しているが、避難者の転居のたびに、担当者が所在を把握する必要があった。これを SAHANA によって、避難者の所在情報を、避難場所別、出身地別などからも常に把握できるようになったという。

■ クラウドの有効性

日本IBM(株)によるコメント [41]

危機的状況で、スピードを求められるときに、すぐに立ち上げることができ、自由に設定できるクラウドは危機管理・事業継続において最適だった。

- インターネット経由を経由して海外のデータセンターからサービスを利用可能だったこと、本番運用環境のみではなく、開発やテスト用の環境も迅速に提供できたこと、インターネット上に開発環境を構築したため、離れた場所での共同開発が可能であったこと等から、様々な観点でクラウドの有効性が認められた。

活用事例： 輸血用血液製剤の安定供給支援

クラウド事業者	日本 IBM(株)
サービス名／サービス種類	LotusLive
有償／無償	無償
利用者	日本赤十字社
利用形態・利用目的	ホスティング
利用内容	輸血用血液情報共有
期間（開始時期）	2011/3/16 から利用開始

40 大河原克行「東日本大震災で活躍した救援情報共有システム「SAHANA」」（2011 年 6 月 29 日）
http://www.asahi.com/digital_sp/cloud_exp/TKY201106280146.html

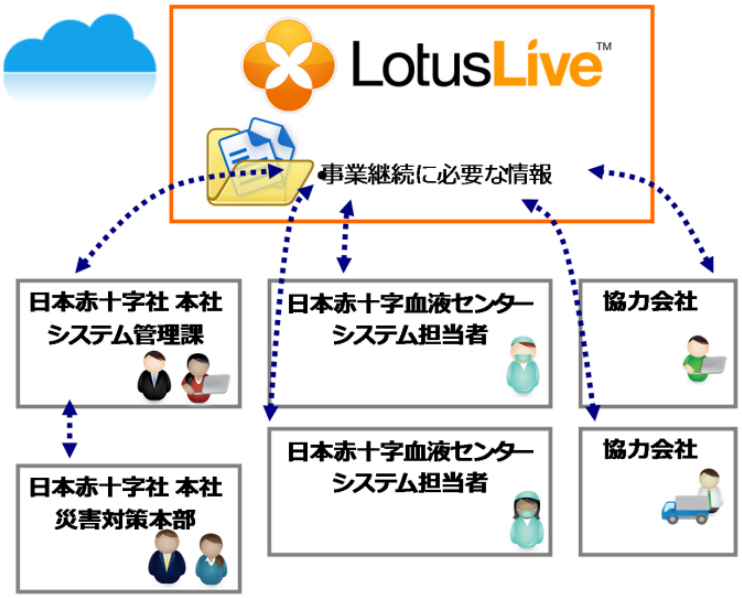
41 日本 IBM への照会結果による。

■　サービスの概要

全国で献血から供給までを支援する「血液事業統一システム」を運用し、血液製剤の医療機関への安定供給を継続。

・　日本赤十字社の「血液事業」にかかわる効率的な情報共有の仕組みを、日本 IBM の提供する LotusLive 環境にて、無償特別プログラムとして早期実現。
・　被災地また社内外の関係者とのコラボレーションを即座に開始することで、震災直後に大量発生した課題を効率的に解決し、関係者との情報共有・仮題の履歴管理などができるようになり、血液製剤の医療機関への安定供給を継続。

図表 72　血液事業統一システムの概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■　サービスの利用実態

日本赤十字社によるコメント [42]

・　日本赤十字社が行う血液事業では、全国を 1 つのシステムでつないで輸血受付から輸血用血液製剤の供給までを管理しています。東日本大震災では被災地におけるネットワーク切断や施設被災状況の把握、資材調達など、解決すべき課題が日を追うにつれて明らかになりました。
・　その中でも、社内外の関係者との情報共有は、当初メールでのやり取りをメインにしていましたが、数日後には整理しきれない状況になっていました。そのようなさなかに

[42] 日本赤十字社　血液事業本部システム管理課　支援係長によるコメント（2012 年 3 月現在）
http://www-06.ibm.com/ibm/jp/provision/no70/pdf/70_interview3.pdf

LoutusLive のニュースを知り、申し込みをさせていただきました。

・ その後は、関係者との情報共有・課題の履歴管理などに活用し、被災地に対する効果的なバックアップを行うことが可能になりました。

■ クラウドの有効性

日本IBM(株)によるコメント[43]

危機的状況で、スピードを求められるときに、すぐに立ち上げることができ、自由に設定できるクラウドは危機管理・事業継続において最適だった。

・ コラボレーションに必要となる一連の機能が SaaS としてすぐに利用可能であったこと、それらをインターネット経由で Web ブラウザから利用できるため、利用者に特定の環境を準備する必要がなく、社外のスタッフにも使用することが可能であったことから迅速性、経済性の面でクラウドの有効性が確認された。また、耐災性、安全性の面からも有効であったと評価できる。

活用事例： 被災動物救護支援サービス

クラウド事業者	富士通(株)
サービス名／サービス種類	Fujitsu Global Cloud Platform FGCP/S5 (オンデマンド仮想システムサービス)
有償／無償	無償
利用者	宮城県緊急災害時被災動物救援本部
利用形態・利用目的	情報共有
利用内容	東日本大震災で被災した保護動物の情報公開を支援する取り組み
期間(開始時期)	2011 年 5 月 2 日から開始

■ サービスの概要

宮城県緊急災害時被災動物救援本部が保有する保護動物のデータ（保護された場所、個体の特徴、写真など）を、富士通のクラウド基盤から提供する「被災動物救護支援サービス」に集約したうえで、日本マイクロソフトがポータルサイト MSN®上で公開している「MSN ペットサーチ」とシステム連携させた。

＜MSN ペットサーチ＞

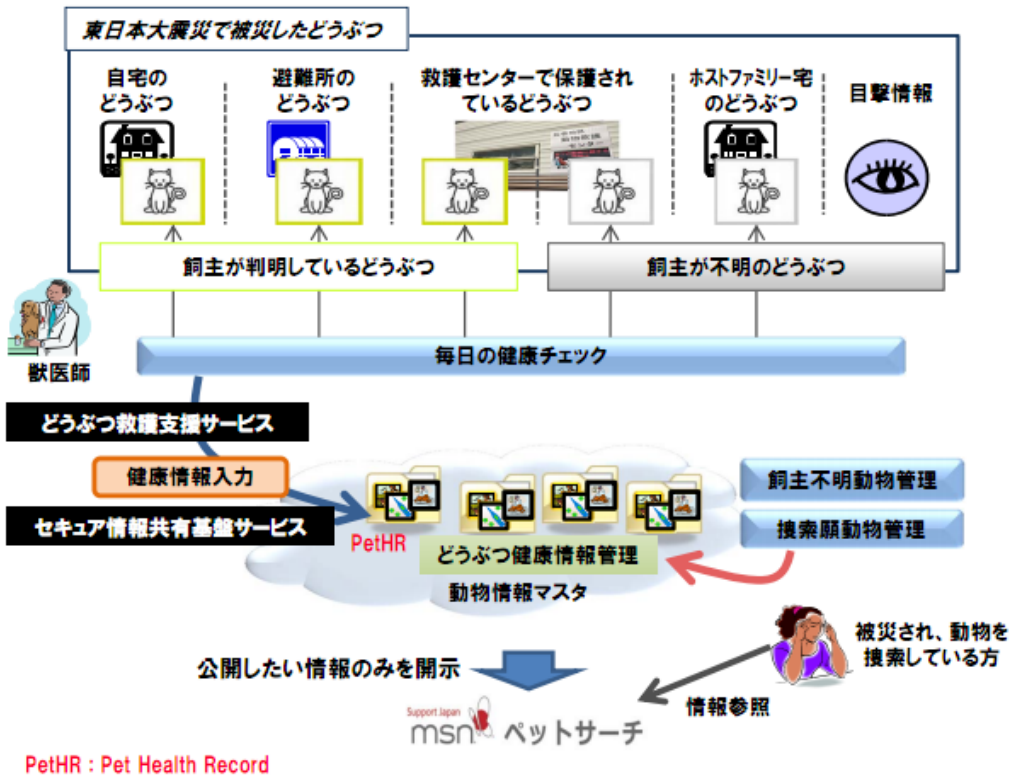
[43] 日本 IBM への照会結果による。

・ 日本マイクロソフトが緊急災害時動物救援本部との連携により、2011 年 4 月 14 日より運営しているサービス。
・ 東日本大震災の影響によって飼い主と離れ離れになった動物の情報を、各動物保護団体より集約して公開することにより、元の飼い主との再会や、新しい飼い主探しを支援している。
・ PC もしくはインターネットが閲覧可能な携帯電話などから無料で利用可能。
・ 日本マイクロソフトのクラウドサービス「Windows Azure™」を基盤としている。

＜被災動物救護支援サービス＞
・ 富士通が宮城県獣医師会向けに、2011 年 5 月 2 日より提供しているサービス。
・ 被災した動物の情報を独自のクラウド基盤に集約し、救援本部による公開を支援している。
・ 富士通のクラウドサービス「FGCP/S5」を基盤としている。

システム連携に際しては、富士通のクラウドサービスを支えるコンポーネントであるセキュア情報共有基盤技術が用いられている。

図表 73 被災動物救援情報システムの概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■ サービスの利用実態

緊急災害時動物救援本部 本部長によるコメント[44]

- 現在、動物保護団体などが保護した動物の情報は、各団体が独自に所有・公開されることが多く、元の飼い主にとっては、自分のペットが無事に保護されているかどうかを確認することが非常に困難でした。また保護団体側も、人員不足などの理由から、保護した動物の最新情報を公開したり、元の飼い主や新しい飼い主を探したりといった「保護した後」の取り組みに十分対応しきれていない現状がありました。
- IT やクラウドを活用することにより、元の飼い主や、新しい飼い主探しが容易になることは、被災地の動物や、被災者の方々の一助となるばかりでなく、動物の殺処分件数の低減という観点からも非常に意義のあることだと考えます。

■ クラウドの有効性[45]

- 迅速性(短期間で構築、サービス開始が可能)、拡張性(利用実態に合わせて能力を拡張することが可能)の面でクラウドの有効性が確認された。

活用事例： 被災者と NPO をマッチングするクラウドサービス

クラウド事業者	富士通(株)
サービス名／サービス種類	SaaS 型 CRMate
有償／無償	無償
利用者	「被災者を NPO とつないで支える合同プロジェクト」(つなプロ)
利用形態・利用目的	支援需給のマッチング
利用内容	被災者のニーズとNPOをマッチングするクラウドサービス。
期間(開始時期)	3 月 28 日からシステム稼働

■ サービスの概要

「被災者を NPO とつないで支える合同プロジェクト（つなプロ)」は、避難所の“実態・実際”を把握するアセスメントを実施し、判明したニーズや課題を、介護・医療・障がい者・外国人・難病患者支援などの分野で高い専門性をもつ NPO 活動とマッチングすることで課題解決をめざすプロジェクト。

[44] http://pr.fujitsu.com/jp/news/2011/07/25-2.html（2011 年 7 月 25 日　富士通プレスリリース）

[45] 富士通への照会結果による。

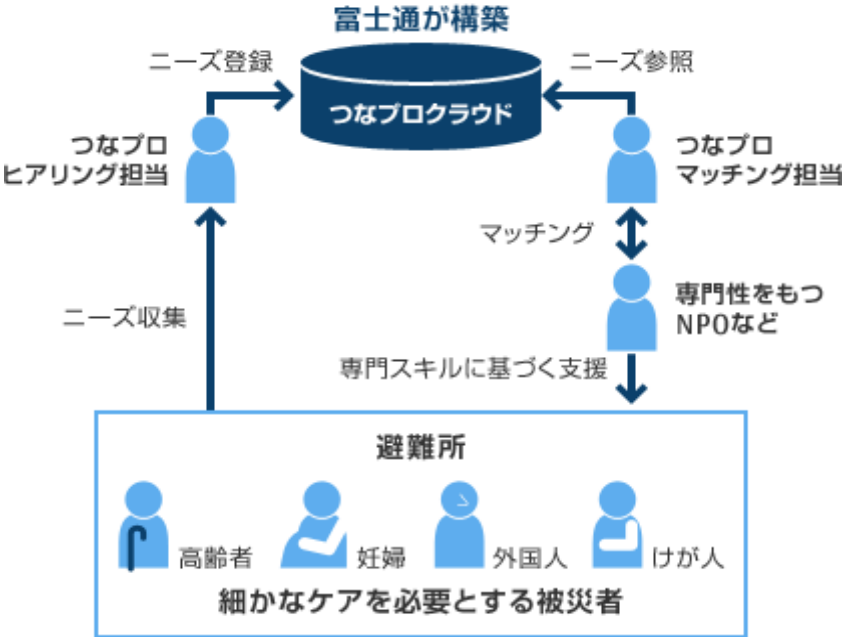
アセスメントにより得た情報をデータベース化する仕組みとして SaaS 型アプリケーションサービス「CRMate」を提供。

＜つなプロ＞

東日本大震災において、複数の NPO と日本財団などが連携して「災害関連死」を防ぐことを目的に設立された。

- 今回の大震災は、被害が極めて甚大であり、避難生活の長期化が予想された。避難所では、妊産婦、軽度の要介護者、精神的要支援者、外国人、障がい者、アレルギー疾患や難病の患者等、様々な配慮、細かな支援を必要とする人々も避難している。
- 救援活動においては、こうした人たちに配慮した支援が必要であり、各分野の専門性を持つ NPO の連携が重要になる。そこで、東北地域の NPO ネットワークの中核的存在である「せんだい・みやぎ NPO センター」と、全国の NPO が連携し、被災者を NPO とつないで支えようという目的で立ち上げられた。
- 被災地において、こうした特別な配慮を必要とする方々のニーズを把握し、専門的支援へとつなげる活動を実施。これまで地域社会において、困難を抱える人たちに様々な社会サービスを開発・提供し、阪神・淡路大震災でも活躍してきた NPO が、それぞれの専門性を活かした支援を行うことで、避難先での死亡や状況悪化の防止・回避を進めている。

図表 74 つなプロの概要（「つなプロクラウド」を使った被災者支援の仕組み）



出所）：http://jp.fujitsu.com/about/csr/feature/earthquake/casestudy/

■ サービスの利用実態

富士通/クラウド戦略統括部担当課長によるコメント[46]

- 3月28日のシステム稼働から4月末までに、つなプロクラウドにはメンバーが足で集めた443件の避難所情報と、966件のニーズ情報が蓄積された。
- 挙がってくる情報はそれぞれのボランティアによって、質の濃淡がある。あらかじめ統一したフォーマットを用意したことで、そうした質のバラつきをなくすことができた。また、クラウド(SaaS)のシステムを使うことで、多数の人間が物理的な距離を超えて、同時に入力することができた。
- 現在は宮城県に限定した活動だが、活動領域が広がってデータ量が増えた場合も、容易にサーバ容量を増設できる。アクセスするユーザの権限管理も自由自在。どちらもクラウド技術の大きなメリット。
- 「サーバの立ち上げなどから始めていたら、半年はかかっただろう。ネット接続さえできればどこからでも開発作業に加われるので、時には名古屋のメンバーに遠隔サポートしてもらった」

■ クラウドの有効性[47]

- 迅速性(短期間で構築、サービス開始が可能)、拡張性(利用実態に合わせて能力を拡張することが可能)の面でクラウドの有効性が確認された。

活用事例： 農山漁村被災者受入れ情報システム

クラウド事業者	富士通(株)
サービス名／サービス種類	SaaS型CRMate
有償／無償	無償
利用者	農林水産省
利用形態・利用目的	情報共有・マッチング
利用内容	「農山漁村被災者受入れ情報システム」の運用により、全国各地の農山漁村に存在する空き家、廃校舎、農林水産業体験施設など受入れ可能な住まい情報、雇用などの受入れ情報を、自治体を通じ被災者に提供。
期間(開始時期)	2011/4/19に運用開始

46 富士通/クラウド戦略統括部担当課長によるコメント:日本経済新聞電子版『被災地の「声」を拾うクラウド 奮闘するエンジニアたち』(2011年5月13日)より引用

47 富士通への照会結果による。

■　サービスの概要

被災者受入れ側の地方公共団体や農林水産業関係団体等が提供する、住まい、雇用の情報、活用できる農地や耕作放棄地の情報等に、被災地域の地方公共団体がインターネットを通じてアクセスできるシステム。

・　農山漁村における住まいおよび雇用などの受入れ情報を収集、管理する農林水産省に協力し、被災者の意向にあわせてスピーディな情報収集、管理を可能とする SaaS 型「CRMate（シーアールメイト）」を提供。
・　受入れ側の地方公共団体、農林水産業・食品産業関係団体等は、随時情報の入力・更新を行う。

図表 75 農山漁村被災者受け入れ情報システムの概要

出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■　サービスの利用実態

農林水産省プレスリリース [48]

□　受入れ側の地域では、地方公共団体、農林水産業・食品産業関係団体、NPO 法人、民間団体等の協力の下、空き家等の住まいの情報、農林水産業関係の雇用の情報、活用できる農地や耕作放棄地の情報等の情報を、より速く、より確実に被災地域へ提供することが可能となります。
□　被災地域の地方公共団体では、被災者の多様な意向を踏まえ、知りたい情報を迅速に把握することができ、効率的できめ細かなマッチングが可能となります。
□　このシステムにより、被災者が被災地域の地方公共団体に受入れ側の地域等の意向を相談した際、意向を踏まえた迅速な情報の提供が可能となります。

[48] 農林水産省プレスリリース「農山漁村における被災者受入れ支援の充実について」より引用 （平成 23 年 4 月 19 日） http://www.maff.go.jp/j/press/nousin/tiiki/110419.html

富士通によるコメント[49]

NPO 様等と連携し、被災者のニーズマッチングや健康調査等、様々な用途で利用された

■ クラウドの有効性[50]

・ 迅速性(短期間で構築、サービス開始が可能)、拡張性(利用実態に合わせて能力を拡張することが可能)の面でクラウドの有効性が確認された。

活用事例： 震災復興支援システム

クラウド事業者	日本マイクロソフト(株)
サービス名／サービス種類	Microsoft Dynamics CRM
有償／無償	無償
利用者	(有)ページワン
利用形態・利用目的	情報収集・共有
利用内容	避難者の情報管理、避難所で必要となる物資の管理
期間(開始時期)	2011 年 3 月

■ サービスの概要

避難所および避難者の情報管理、避難所で働くボランティアの管理、緊急支援物資の管理などの情報を体系的に整理し、避難所の運営をスムーズにできるソリューション「震災復興支援システム」を無償提供。企業で使われている CRM（顧客関係管理）のクラウドサービスである「Microsoft Dynamics CRM Online」というソリューションを利用することで、被災地域の避難所運営に最適化して活用することができる。

■ サービスの利用実態[51]

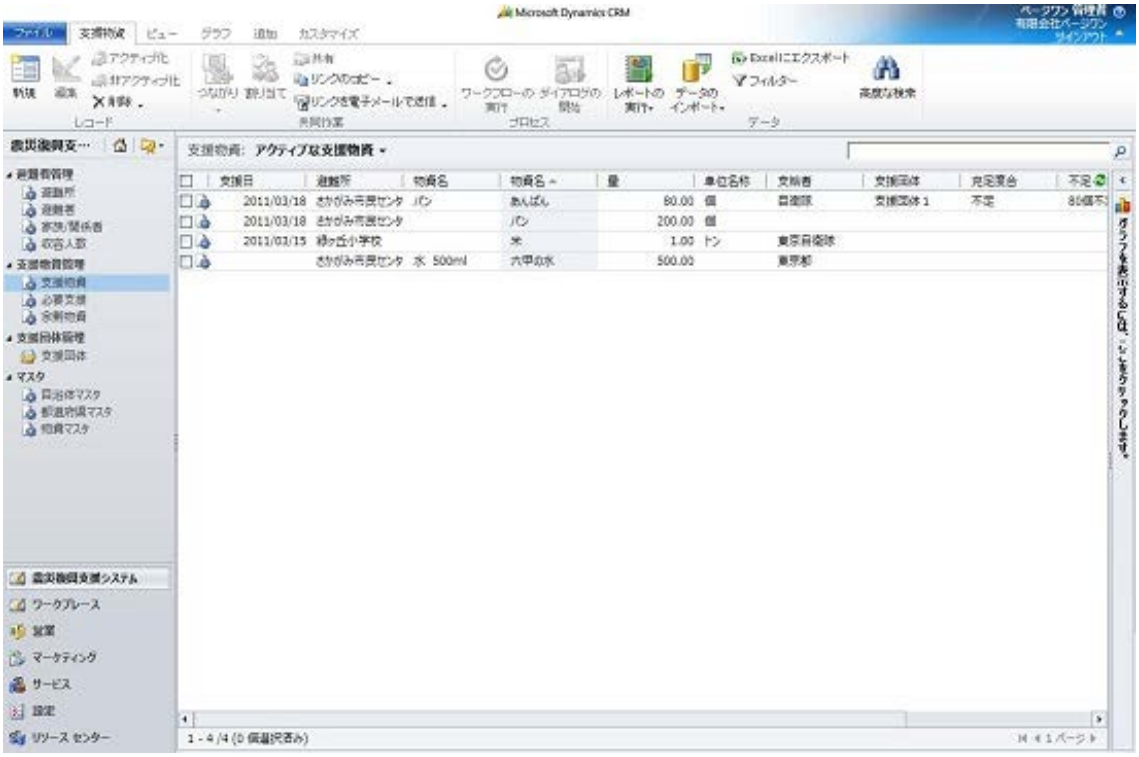
避難所の状況の移り変わりが激しかったため、避難所から情報の管理者への情報伝達が十分に行われず、システムへの情報登録があまり行われなかった。この結果、活発に利用されるに至らなかった。

49 富士通への照会結果による。
50 富士通への照会結果による。
51 (有)ページワン代表取締役への照会結果による。

■　クラウドの有効性

避難所で情報伝達に係る人手不足という運用上の問題のために、実際に十分に活用されることはなかったが、迅速にサービスが開始されたことはクラウドの有効性として評価できる。

図表 76 震災復興支援システムのサンプル画面:支援物資一覧



出所）マイクロソフト Web サイト http://www.microsoft.com/japan/presspass/detail.aspx?newsid=3978

③ 行政情報提供サイトの拡張

活用事例：　クラウド環境にミラーサイトを構築し、アクセス集中に対応

クラウド事業者	日本 IBM(株)
サービス名／サービス種類	IBM Smart Business Cloud
有償／無償	無償
利用者	浦安市
利用形態・利用目的	サーバミラーリング

利用内容	災害情報
期間(開始時期)	2011/3/18 からクラウド上で稼働

■　サービスの概要

災害対策 web サイトのミラーサイトをクラウド環境に構築することにより、アクセス集中に対応。災害情報の提供を行った。

- 震災に伴い液状化現象で甚大な被害を受けた浦安市では、迅速に災害対策 Web サイトを立ち上げ、日々の生活に直結するガス、水道、下水道、道路の復旧見込みなどの情報をタイムリーに提供していた。
- しかし日を追うごとにアクセスが増え、レスポンスの遅延、あるいは一部アクセス不能という事態が発生し、災害対策ページを継続的に運用するための対策の必要に迫られた。
- そこで、日本 IBM が無償提供していた IaaS のホスティングサービスの利用を相談した。
- 日本 IBM 側では事前にクラウド環境にミラーサイトの稼働環境を整備し、正式申し込みと同時にミラーサイトをオープンした。

図表 77 ミラーサイトの構築

※当時の Web サイトのイメージ

出所）：http://www-06.ibm.com/ibm/jp/provision/no70/pdf/70_interview3.pdf

■　サービスの利用実態

浦安市　総務部　CIO補佐によるコメント[52]

「被災自治体へのボランタリーな提案を迅速に受けたことにより、混乱に至る前にミラーサイトを構築できました。このたびパブリッククラウド環境を活用したことで、対応システムの早期構築も実現できるなど意義を実感できました。今回の震災を通して、震災当初の市民への情報提供、罹災証明の発行など、災害への対応において情報システムが不可欠であることが再認識されました。事業継続という点から、災害体制

[52] http://www-06.ibm.com/ibm/jp/provision/no70/pdf/70_interview3.pdf（2012 年 3 月現在）

をさらに高めて継続的な情報システム運用を実現したいと考えます。」

■ クラウドの有効性

日本IBM(株)によるコメント[53]

ミラーサイトの迅速な稼働により、市民の方々に対して刻々と変化する情報をタイムリーに発信し続けることが可能になった。クラウドの持つ利便性や有効性が証明された。

・ インターネットを経由して、リモートのデータセンター上にわずか数分で仮想サーバを立ち上げることができたこと、サービスを提供するデータセンターが海外であったため、地震の影響を全く受けることがなかったこと等から、迅速性、耐災性の面でクラウドの有効性が確認された。

活用事例： 「東日本大震災 子どもの学び支援ポータルサイト」にクラウド型情報基盤サービスを提供

クラウド事業者	日本ユニシス(株)
サービス名／サービス種類	U-Cloud™ IaaS、NeXtCommons
有償／無償	無償
利用者	各地方公共団体、教育委員会、学校、企業、NPO 等
利用形態・利用目的	支援需給のマッチング
利用内容	文科省 東日本大震災 子どもの学び支援ポータルサイト
期間(開始時期)	2011 年 4 月開始

■ サービスの概要

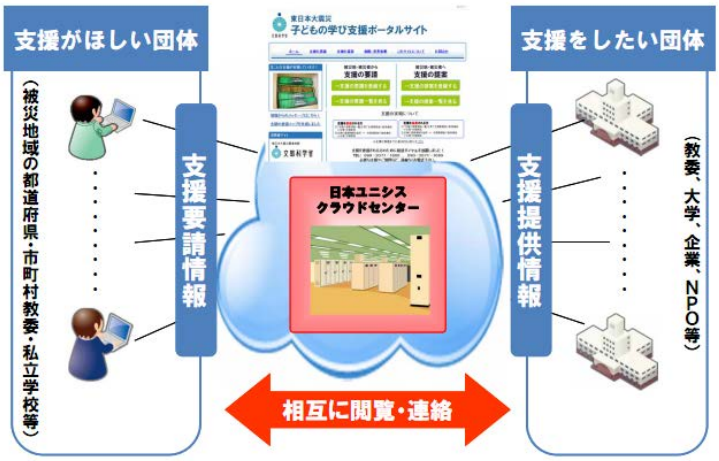
日本ユニシス(株)とユニアデックス(株)は、被災地域の復興支援の一環として、文部科学省の「東日本大震災 子どもの学び支援ポータルサイト」にクラウド型情報基盤サービスを提供。

・ 「教職員を派遣してほしい」、「学用品が足りない」といった被災地域からの支援要請に対し、人的支援や物的支援が可能な申し出を相互に結びつけるマッチングサイト。
・ 被災地域で現在どのような支援を必要としているのかを各地方公共団体や教育委員会などを通じて掲載。また、支援の検討をしている地方公共団体・教育委員会・学校・企業・NPO などが、どのような支援を提供することができるのかについて登録。

[53] 日本 IBM への照会結果による。

・ ユニアデックスのクラウド型情報基盤サービス「NeXtCommons®（ネクストコモンズ）」、日本ユニシスのクラウドサービス「U-Cloud™ IaaS」を利用して、サイトの開設・立ち上げを無償で支援

図表 78 子どもの学び支援ポータルサイトの概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■ サービスの利用実態

文部科学省による発表記事 [54]

「多くの方に子どもの学び支援サイトにアクセスいただく中で、多数の支援が実現してまいりました。」

（参考）ポータルサイトの実績（平成 24 年 3 月 18 日現在）

- □ 累計ページビュー：1,211,396 ページ
- □ 累計訪問件数：342,709 件
- □ 支援の提案件数：917 件
- □ 支援の要請件数：402 件
- □ 総マッチング件数：2,257 件

■ クラウドの有効性 [55]

・ 震災発生後(3 月 11 日)に被災地支援の内容を検討し、ポータルサイトを運用することを決めてから開始(4 月 1 日)までの短期間で、サイト構築およびサービス開始に至ったことから、迅速性の面で有効であった。

・ また、ネクストコモンズというシステムを使用し、デザイン変更や、ツィッターやグーグルマップなどとの連動など、多種多様な機能をもったモジュールがあらかじめ用意されていたの

[54] 文部科学省『東日本大震災における「子どもの学び支援」に関するWebサイトを通じた情報発信等について』（平成 24 年 3 月 19 日）http://www.mext.go.jp/b_menu/houdou/24/03/1318834.htm

[55] 文部科学省担当者への照会結果による。

で、新たな機能追加についてストレスを感じることなく実現できたため、拡張性の面からも評価できる。

④ 被災企業等の緊急情報発信・業務処理

活用事例： アクセス急増した震災情報システムに IaaS 環境で迅速に対応

・ クラウド事業者	富士通(株)
・ サービス名／サービス種類	Fujitsu Global Cloud Platform FGCP/S5 (オンデマンド仮想システムサービス)
・ 有償／無償	無償
・ 利用者	ESRI ジャパン(株)
・ 利用形態利用目的	ホスティング
・ 利用内容	アクセス急増した震災情報システムに対応
・ 期間(開始時期)	2011/3/18 申し込み(2011/3/20 から運用)

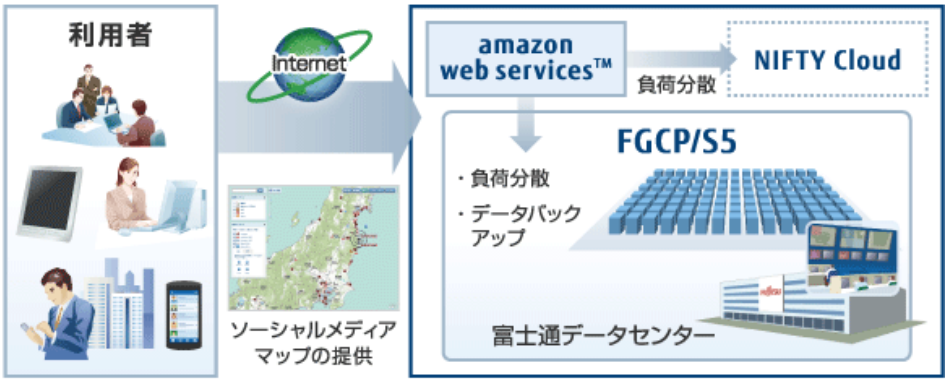
■ サービスの概要

急増するアプリケーションユーザからのアクセスに、クラウドサービスによる FGCP/S5 で対応。複数のサービスにクラウドサービスを組み合わせ、予測できない負荷急増のリスクを回避した。

＜導入の経緯＞

- ESRI ジャパンは、米国 ESRI 社の地理情報システム（GIS）製品の日本における総販売代理店。2011 年 3 月 11 日の東日本大震災直後、同社は EMT（東北地方太平洋沖地震緊急地図作成チーム）の一員として地図作成活動を支援し、また同社ホームページ上で震災関連の各種地図やソーシャルメディアマップを公開するなど、震災復興への積極的支援を続けている。
- とりわけソーシャルメディアマップの一般向け無償公開がネット上で大きな反響を呼んだ。震災後、このソーシャルメディアマップを公開したことがメールマガジンなどにより広く紹介され、それまで利用している Amazon に加えて、急増するアクセスに余裕を持たせる対応を迫られた。
- 震災 1 週間後に富士通のクラウドサービス選定、「東日本大震災クラウド／保守サービス特別ご支援プログラム（無償）」を利用。その 2 日後には複数のクラウド上に復興支援の無償 GIS アプリケーションを載せたシステムが動き始めた

図表 79 ESRI Japan への提供システム



【ESRIジャパン株式会社様 システム概要図】

【課題と効果】

1	震災後、無償公開したGISアプリケーションへのアクセス急増に、迅速かつ柔軟に対応したい	→	クラウド利用申し込み2日後に運用を開始できた
2	利用ユーザー増加時も、アプリケーションの動作速度を保つ必要がある	→	スペック保証のクラウドサービスを利用し、ユーザー急増時の動作速度低下を回避
3	国内データセンターが被災する可能性を限りなくゼロに近づけたい	→	国内・海外6拠点のデータセンターを活用するシステムでセキュリティは万全

出所）http://jp.fujitsu.com/solutions/cloud/casestudies/esrij/?inside=top-news

■ サービスの利用実態

ESRIジャパン　システムソリューション推進第 1G部長によるコメント [56]

・とくに富士通のクラウドにはデータのバックアップも担っていただくことになりました。一定のスペックを保証するなど性能重視の富士通クラウドは『今後、どれくらい負荷が高まるか見通せない』という状況において高く評価できました。また仮想サーバの管理画面が分かりやすく使いやすい点、データセンターが地震・津波リスクを抱える国内だけでなく海外 5 拠点で展開している点も選定の大きな理由でした

・GIS のアプリケーションは、それを動作させるハードウェアのスペックを慎重に見積もる必要がありますので、それをクラウドの柔軟性でフォローする有効性については、頭では理解しているつもりでした。その上で今回、2 日間でクラウドサービスの新規展開を経験し、弊社スタッフ全員があらためてその威力を実感しました

[56] http://jp.fujitsu.com/solutions/cloud/casestudies/esrij/?inside=top-news （2012 年 3 月確認）

富士通によるコメント[57]

- 地理情報システム等、震災関連サービスを提供される企業様を中心に、ある程度、活用戴いた。

■ クラウドの有効性[58]

・ 迅速性（短期間で構築、サービス開始が可能）の面でクラウドの有効性が確認された

活用事例： 被災地向け安否確認・Web 会議の提供

・ クラウド事業者	富士通(株)
・ サービス名／サービス種類	Web 会議 SaaS
・ 有償／無償	無償
・ 利用者	自治体、企業、非営利団体等
・ 利用形態利用目的	Web 会議
・ 利用内容	企業等の災害対応のための情報インフラ
・ 期間(開始時期)	2011/3/17～2011/7/31

■ サービスの概要

被災した商工会議所、商工会連合会・商工会、団体中央会及びその会員企業向けに、Web 会議を活用した支援アプリケーションをクラウド環境に搭載、提供。

＜システム概要＞

Web 会議サービス（SaaS 型、パッケージ）「JoinMeeting」

・ いつでも、どこからでも、インターネットを経由して簡単に Web 会議を行なえる SaaS 型サービス。

・ パソコン、ヘッドセットなどの会話ツール、Web カメラだけで手軽に利用できる。

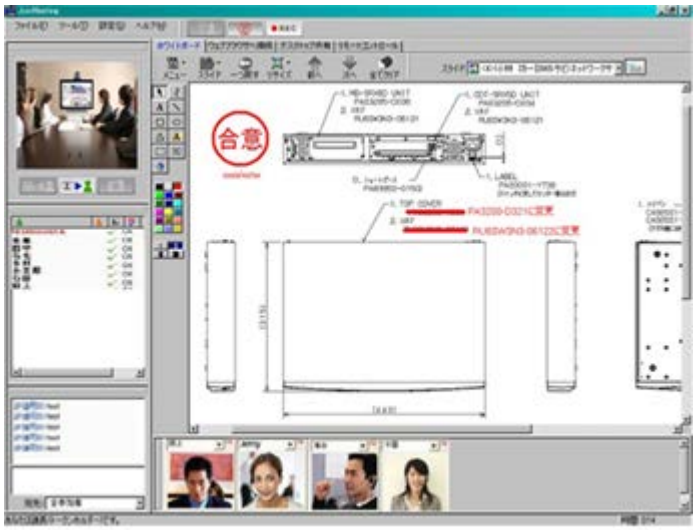
■ サービスの利用実態

富士通によるコメント[59]

- 被災された商工会議所・商工会等で利用戴いた。
- 非常に役だった。

57 富士通への照会結果による。
58 富士通への照会結果による。
59 富士通への照会結果による。

図表 80 Web 会議 SaaS の概要



「JoinMeeting」のクライアント画面イメージ

出所）：http://fenics.fujitsu.com/networkservice/joinmeeting/
http://fenics.fujitsu.com/casestudies/2010/nidec-copal/?from=bottomMenu

■ クラウドの有効性 [60]

・ 迅速性（短期間で構築、サービス開始が可能）の面でクラウドの有効性が確認された。

活用事例： 大学連携高度教育基盤システム

クラウド事業者	ニフティ(株)
サービス名／サービス種類	ニフティクラウド
有償／無償	無償
利用者	大学 e ラーニング協議会/各大学
利用形態・利用目的	教材の相互活用
利用内容	クラウド上で各大学の講義コンテンツを共有。クラウド上の e-ラーニング環境も活用。
期間（開始時期）	2011 年 4 月 22 日開始

■ サービスの概要

被災地支援の取り組みとして、e ラーニングによる大学向けの講義、教材および大学の単位認定の支援などを行う高度教育基盤の提供を行った。

60 富士通への照会結果による。

＜経緯＞

・ 被災地の大学では、校舎等の損壊や計画停電・交通機関の制限等により、開講時期の遅れや授業回数の確保が困難になるなど、新年度以降の学生の学習に支障が出ることが懸念されている。
・ この状況を踏まえ、大学 e ラーニング協議会、ニフティ、住商情報システム(株)（SCS：当時。現 SCSK）は、被災学生に質の高い教育機会を提供するため、各団体、各社の持つ技術・ノウハウを集約し、全国の大学で相互に活用可能な e ラーニングによる高度教育基盤を構築。

＜システム＞

・ 大学 e ラーニング協議会が全体の取りまとめを行い、参加大学が保有する既存講義コンテンツ、授業用の教材およびクラウド上の e ラーニング環境自体を自由に利用できる仕組みを構築する。また、問い合わせに応じて e ラーニングを活用した授業実践手法、学生の自学自習支援手法などのノウハウを提供。
・ ニフティは、e ラーニングのシステム基盤として『ニフティクラウド』を提供。『ニフティクラウド』のネットワーク、ストレージ、サーバーリソースを活用することで、全参加大学に安定した講義を実施するための環境を整えた。
・ SCS は、ユーザの認証や管理などを一元化し、「なりすまし受講」や「不正利用」を防ぐ仕組みとして、SCS の持つクラウド統合認証サービス「SCS CLIP IAS」および、自社で培ったセキュリティ技術・ノウハウを提供。

＜SCS CLIP IAS について＞

CA Technologies の「CA Arcot WebFort」をベースとした SCS のクラウド統合認証サービス。CA Technologies の協力のもと、大学 e ラーニング協議会に提供。

・ 今回の無償提供では、CA Technologies の「復興支援 Arcot 無償プログラム」を活用し、1 年間、被災大学や援助大学に対して提供。
・ “多要素認証”機能である「ArcotID」を備えており、これを PC やスマートフォン、iPad などの端末にインストールすることにより、ハードウェア・トークン等の機器の配布・管理・持ち運びの負荷を負うこと無く、強固なセキュリティに保護されたリモート・アクセスが可能になる。
・ クラウド型サービスであるため、運用負荷を軽減し、ユーザ数の増減にも迅速に対応できる。

■ サービスの利用実態 [61]

「大学連携高度教育基盤システムは、4 月 15 日に関係者が東京に集まり構築を開始し、4 月 22 日にオープンしました。1 週間もない準備時間のなかで、多くの教材があつまり、また骨太のクラウド環境が動きだし、強力な認証システムも準備が完了しました。」

■ クラウドの有効性 [62]

- 迅速性、拡張性、耐災性、安全性の面でクラウドは有効であった。ただし、耐災性、安全性の面では資料を一定基準に基づいて公開するなどの対策が必要である。
- 経済性については、安いクラウドほど障害を起こしやすい傾向があることに留意が必要である。

活用事例： 取引先企業の被災状況や工場稼働状況の確認

クラウド事業者	日本ユニシス(株)
サービス名／サービス種類	購買部門向け SaaS サービス「eSupplierStation」
有償／無償	無償
利用者	震災や停電の影響で資材や部品調達が難航し、取引先の状況確認が必要な企業や団体
利用形態・利用目的	情報収集・共有
利用内容	取引先企業の被災状況や工場稼働状況の確認。
期間(開始時期)	最大 3 ヶ月間(平成 23 年 8 月末日まで) 受付期間:平成 23 年 4 月 26 日より 7 月末日まで

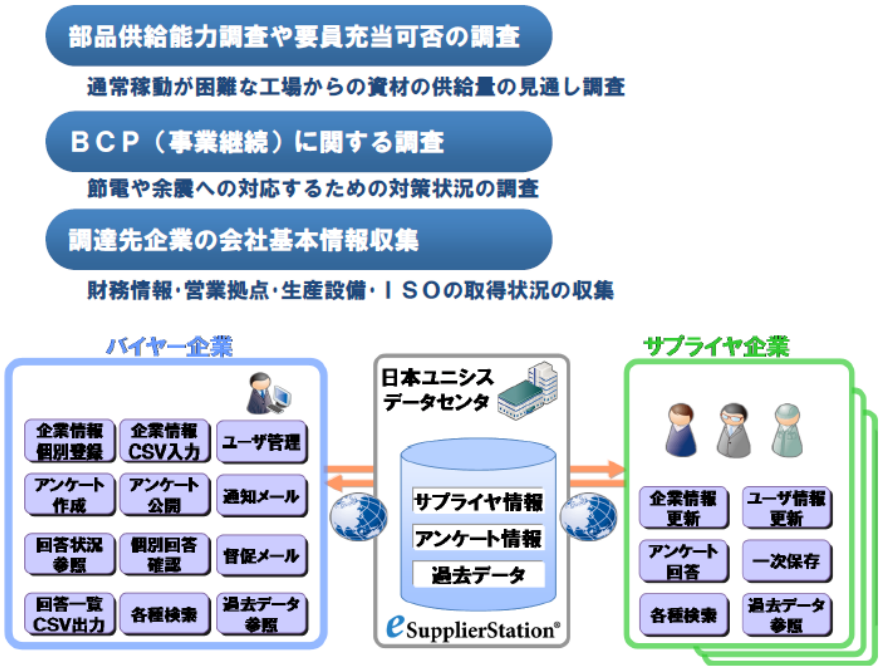
■ サービスの概要

購買部門が実施している取引先への調査やアンケートを効率的に実施し、サプライヤー（供給者）からの情報を有効活用するための取引先情報共有サービス。

- 取引先企業の被災状況や復旧時期の確認、計画停電による工場稼働状況の確認や部品供給能力の調査、事業継続計画(BCP)の内容確認などの情報収集を効率的に行うことができ、生産活動の予測が可能になる。

61 信州大学教授「大学高度教育基盤システムの導入について」より引用(2012 年 3 月現在)
http://www.uela.org/htdocs/pdf/NewsLetter/no3.pdf
62 ニフティへの照会結果による。

図表 81 eSupplierStation の概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■ サービスの利用実態 [63]

サプライヤ企業向けのアンケートシステムとして、震災の影響を確認することなどに利用された。

■ クラウドの有効性

・ 迅速性、拡張性、耐災性、安全性の面で、クラウドは有効であると日本ユニシスの担当者は評価している。

活用事例： クラウド型データ保管・共有サービス

クラウド事業者	(株)日立システムズ
サービス名／サービス種類	クラウド型データ保管・共有サービス「セキュア保管庫」
有償／無償	無償
利用者	自治体、企業等
利用形態・利用目的	データ保管・共有

[63] 日本ユニシスへの照会結果による。

利用内容	サーバ、PC の重要データを保存し共有できる場所を提供。
期間(開始時期)	2011/4/7 開始

■ サービスの概要

・ パソコンやサーバで保管するデータを、データセンター内に安全に一時保管・共有。

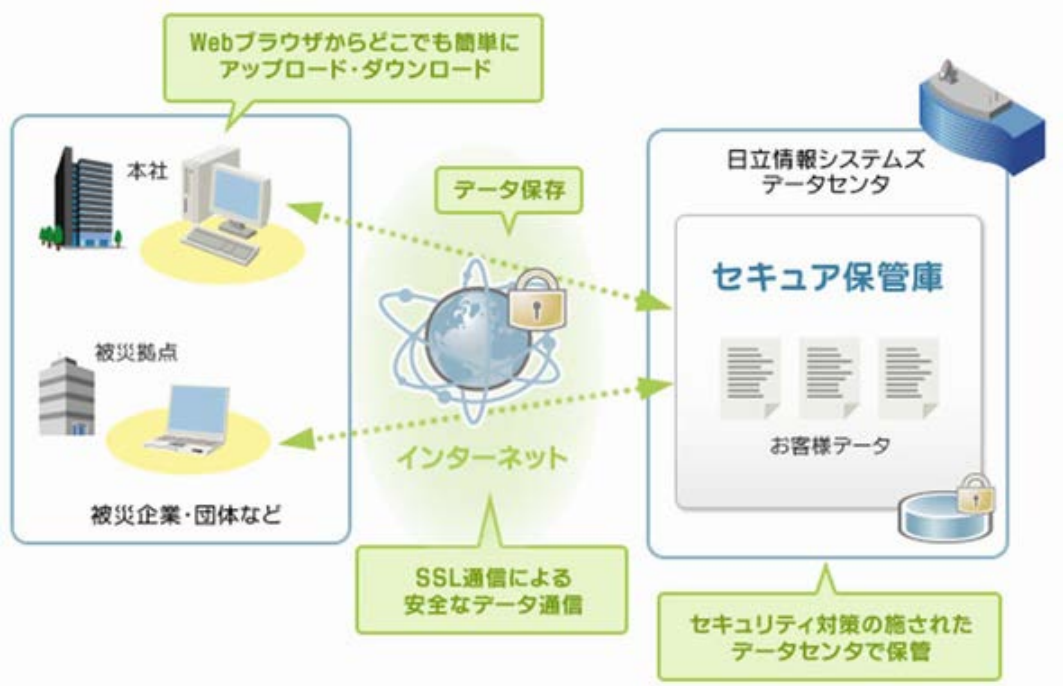
・ Web ブラウザがあれば利用可能。

・ パソコンの故障などによるデータ消失への対策として利用可能。

■ サービスの利用実態 [64]

・ クラウド上でファイルの一時的な保存が可能になり、自治体や企業等で、ある程度利用された。

図表 82 セキュア保管庫の概要



出所)総務省「東日本大震災に関するクラウドサービス活用事例集」(2011 年 11 月 4 日)

■ クラウドの有効性

日立システムズ(株)によるコメント

クラウド上でデータ共有することで、万が一再被災があったとしてもデータの消失を防げる。

・ データの保全が図られることから、耐災性の面でクラウドの有効性が評価できる。

64 日立システムズへの照会結果による。

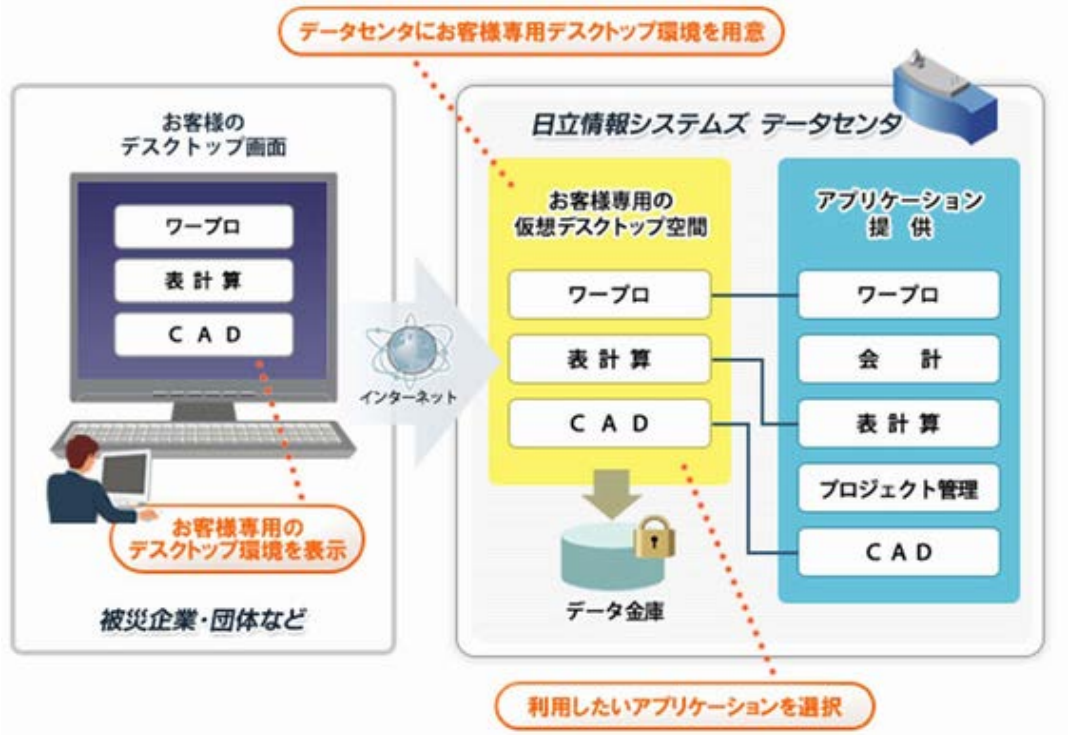
活用事例： 仮想デスクトップ提供 Dougubako（どうぐばこ）

クラウド事業者	(株)日立システムズ
サービス名／サービス種類	DaaS サービス「Dougubako（どうぐばこ）」
有償／無償	無償
利用者	自治体、企業等
利用形態・利用目的	情報保存・共有
利用内容	インターネットを通じて、日立情報データセンターに設置したサーバのハードディスク、メモリを利用できるクラウド型のサービス。情報保存・共有ための臨時システムとして利用。
期間（開始時期）	2011/4/7 開始

■ サービスの概要

- データセンター内に構築された顧客専用の仮想デスクトップ空間を提供。
- 作成したデータはデータセンター内の「データ金庫」にてセキュアに保管。
- 顧客の利用したいアプリケーションを選択して利用可能。

図表 83 DaaS サービス「Dougubako」の概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■ サービスの利用実態 [65]

・ パソコン本体と共にシステムを提供し、提供から即業務の再開が可能となったことから、大いに利用された。

■ クラウドの有効性

日立システムズ(株)によるコメント

・ クラウド側でオフィス系ソフトが準備されているため、提供からすぐに利用できる点が評価が高かった。
・ また万が一再被災があったとしても、データはクラウド上に保管されるため、パソコン・端末の損壊にも耐えられる他、事務所が倒壊しても自宅などからデータ・システムへのアクセスが可能。

・ 上記のコメントから、迅速性、耐災性の面からクラウドの有効性が確認された。

活用事例： 仮想サーバの無償提供

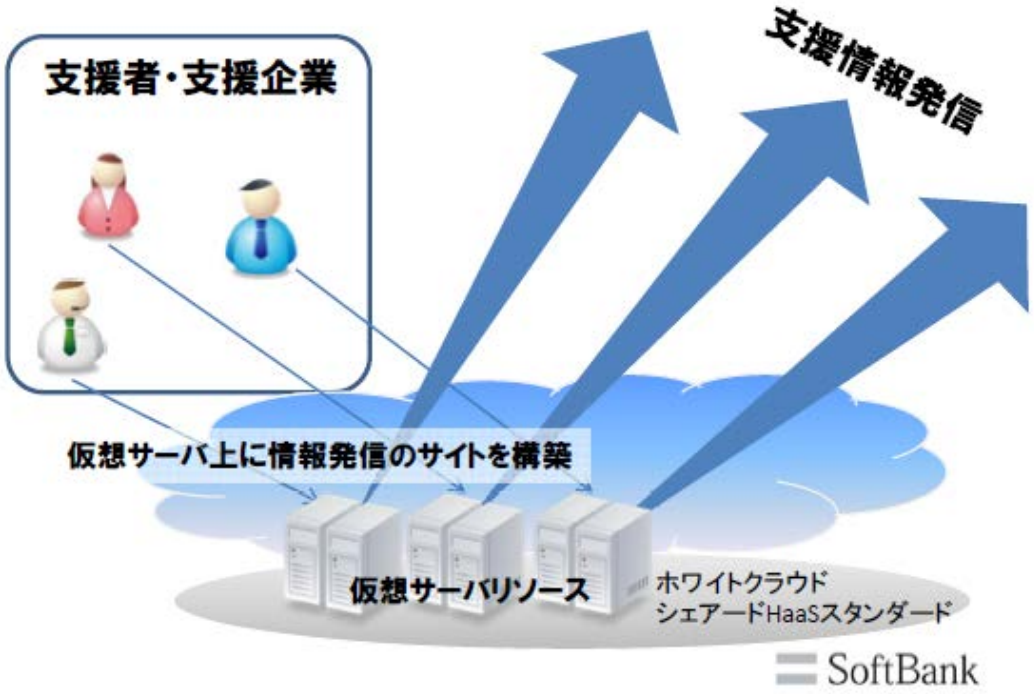
・ サービス提供者	ソフトバンクテレコム(株)
・ サービス名／サービス種類	ホワイトクラウド シェアード HaaS スタンダード
・ 有償／無償	無償
・ 利用者	助けあいジャパン
・ 利用形態利用目的	ホスティング
・ 利用内容	仮想サーバのリソースを無償で提供
・ 期間（開始時期）	2011/3/14～

■ サービスの概要

・ 復興支援等の情報発信サイトの新規構築や、既存の公的情報提供サイトのアクセス集中対策目的に、「ホワイトクラウドシェアード HaaS スタンダード」を 3 月 14 日から無償で提供開始。
・ 義援金募集活動サイト、ボランティア支援ポータルサイト、輪番停電情報発信サイト、安否確認情報サイトなど、19 団体様、33VM(仮想マシン)が被災者支援・災害情報提供に利活用。

65 日立システムズへの照会結果による。

図表 84 ホワイトクラウド シェアード HaaS の概要



出所）総務省「東日本大震災に関するクラウドサービス活用事例集」（2011 年 11 月 4 日）

■ サービスの利用実態

助けあいジャパン担当者によるコメント [66]

> 非常に役だった。発災後、迅速に支援決定、導入でき、用途拡大に応じた拡張が容易だった。災害時向け支援として、無償で利用させていただけた。

ソフトバンクテレコム担当者によるコメント [67]

> 非常に公益性の高い通信事業者として広くかつ迅速に情報共用の場を提供することは使命の一つでもありました。クラウドプラットフォームを、この目的のために無償提供できたことは社会貢献の意味も込め、弊社にとって非常に役立った事例でした。

■ クラウドの有効性 [68]

・ 迅速性、拡張性をはじめ、様々な面で、クラウドの有効性が発揮された。

66 助けあいジャパンへの照会結果による。
67 ソフトバンクテレコムへの照会結果による。
68 助けあいジャパン及びソフトバンクテレコムへの照会結果による。

2.3.2. 被災団体の対応実態の分析

被災した地方公共団体における情報システムの復旧・復興に向けた取組を整理し、利用者及び利用者の IT をサポートする立場の視点から、クラウド活用の実態を分析した。

図表 85 東北 4 自治体の危機的事象と被害状況の事例

		国見町 （福島県）	多賀城市 （宮城県）	陸前高田市 （岩手県）	山田町 （岩手県）
危機的事象		・震度 6 強	・震度 5 強 ・津波 4.6m	・震度 5 強～6 弱 ・津波 21.5m	・震度 5 弱 ・津波 ・火災
被害状況	庁舎	使用不能→移転 地震動で一部損壊、周囲の液状化で使用不能	被害なし	使用不能→移転 津波で4階まで浸水	使用不能→修復 津波で大破
	電力	当日は停電 翌日から復旧	三日間停電	三日間停電	3/15 から発電機で庁内へ給電開始
	データ	被害なし	被害なし	被災 一部被災ディスクから復旧	被災 一部被災ディスクから復旧
	外部ネットワーク	3/22 に移転庁舎で利用可能に	3/17 まで インターネット不通	3/29 に衛星携帯で、3/31 に通信衛星でアクセス可能に	4/14 に庁内からインターネットへのアクセスが可能に
	人材	被害なし	被害なし	被災。前々任が引き継ぎ。市外から支援受入	負傷するも数日後に復帰。

出所）東日本大震災被災地自治体 ICT 担当連絡会「東日本大震災と自治体 ICT」セミナー資料及び公開情報をもとに作成

図表 86 東北 4 自治体の位置関係

対応事例： 国見町

■ 危機的事象・被害状況

- 震度 6 強。
- 庁舎が損壊、周囲は液状化（庁舎の耐震補強計画は22年度に策定され、工事が23年度に予定されていた）。
- ホームページはデータセンターにハウジングしていたため被害なし。

■ 復旧に向けた対応

- 文化センターへ、役場機能の移転を決定（電源工事の業者、部材の確保に奔走）。
- 翌々日（3/13）からシステム復旧に向け本格始動。
- 2 週間後（3/25）から、全業務を再開。

■ 復興に向けた対応

- 基幹系システムのクラウド化。
- 庁舎とすべての主要施設を、光ケーブルに加え、無線で接続。

図表 87 国見町役場の被害と復旧

当日(3/11)　　移転後（3/25）

出所）東日本大震災被災地自治体 ICT 担当連絡会「東日本大震災と自治体 ICT」セミナー資料

対応事例：　多賀城市

■ 危機的事象・被害状況

・ 震度 5 強。津波で市域の 3 分の 1 が浸水。死者 188 名。

・ 情報システムは仙台のデータセンターで運用していたため、被害なし。庁内のサーバも免震床で被害なし。

・ NTT 基地局被災により、インターネットが数日不通。ホームページの運用が途絶。

■ 復旧に向けた対応

・ ネットの通じる個人宅からホームページの情報を更新。支援物資が届くようになる。

・ 被災者向け相談窓口設置に伴って、業務横断的に、相談履歴を一元管理するシステムを職員が 5 日間で構築。

・ 市民対応窓口の環境に、無線 LAN を導入。

※3/11 時点の住民記録データを隔離保存しなかったことは反省点。

■ 復興に向けた対応

・ ホームページの更新もできる衛星携帯電話を調達。

・ データの遠隔地保存を検討中。

図表 88 多賀城市で稼働している震災関連システム等

業務名	稼働日	ソフト等	開発元
り災証明発行	4/20	Access	(株)パスコ様
義援金管理	4月末	Access	日本電気(株)様
災害援護資金貸付	未定	未定	未定
仮設住宅	4/1	Excel	職員
住宅の応急修理	4/25	Excel	職員
被災者相談窓口 (被災者生活再建支援)	4/1	オープンソース	職員

出所）東日本大震災被災地自治体 ICT 担当連絡会「東日本大震災と自治体 ICT」セミナー資料

対応事例： 陸前高田市

■ 危機的事象・被害状況

- 震度 5 強～6 弱。倒壊はなし。津波で庁舎 4 階まで浸水。
- 情報システム、データは津波で被災。データは一部被災ディスクから復旧できた。
- NTT 局舎が津波で被災し、電話、インターネットが不通。

■ 復旧に向けた対応

- 情報システムの現任が被災したため、前の前の職員が引き継ぎ。また、名古屋市の情報システム職員が長期サポート
- 衛星携帯電話 2 台を職員 2 名が 24 時間はりついて外部と交信。事実上のライフライン。
- 仮庁舎におけるサーバルームを、情報システム担当一人で設計、調達、構築。
- システム不具合が頻発。ほとんどが電源が不安定なことに起因。自家発の併用、UPS や CVCF の増設で対応。

■ 復興に向けた対応

- データバックアップの拡充（クラウド活用など）

図表 89 被災後のサーバルーム（ここから可能な限りデータを取り出した）

出所）東日本大震災被災地自治体 ICT 担当連絡会「東日本大震災と自治体 ICT」セミナー資料

対応事例： 山田町

■ 危機的事象・被害状況

- 震度 5 弱。津波、火災で壊滅的被害。
- 庁舎地下に設置していた情報システム、発電機等はすべて破壊。
- データは一部被災ディスクから復旧できた。

■ 復旧に向けた対応

- 「電気がないなら、電気を作れ！」の課長の指示で、担当者が自家用車で盛岡に行き、大型発電機を調達。
- 6 台の発電機を調達し、18 リッター缶を毎日 20 缶給油。
- 電源不足で、昼は被災者支援、夜は内部業務を稼働。3 ヶ月この状態が続く。
- 衛星通信、3G 回線でインターネット接続
- データは二次利用できるように USB メモリで保存。外部とのデータ交換に、オンラインストレージを利用。

図表 90 山田町_役場庁舎被害（情報システム、自家発は地下にあったため破壊された）

出所）東日本大震災被災地自治体 ICT 担当連絡会「東日本大震災と自治体 ICT」セミナー資料

2.4. 東日本大震災に関するクラウドサービスの有効性の検証結果

■ 東日本大震災に際して、被災者・被災企業やその救援・支援にあたる行政やボランティア組織に対して提供された様々なサービスにおいて、クラウドが有効活用されていた。

- 情報共有・流通基盤
- 被災者救援活動の情報インフラ
- 行政情報提供サイトの拡張
- 被災企業等の緊急情報発信・業務処理

■ 東日本大震災に際して利用されたクラウドサービスでは、特に「迅速性」の面で有効性が確認された。また、「拡張性」や「耐災性」についても有効性が評価できる事例が多数みられた。

［有効性の観点］

- 迅速性（短期間で構築、サービス開始が可能）
- 拡張性（利用実態に合わせて能力を拡張することが可能）
- 経済性（必要なリソースだけ利用することができる、供給側のコスト負担が限定的）
- 耐災性（災害に強い）
- 安全性（情報セキュリティに優れている）

図表 91 分析対象としたサービスの観点別の有効性評価

用途区分	活用事例	有効性の観点				
		迅速性	拡張性	経済性	耐災性	安全性
① 情報共有・流通基盤	岩手県の安否情報 Web サイト	○			○	
	在宅勤務による事業継続				○	
	被災地医療に生かされた在宅医療クラウド	○	○			
	被災した企業の企業活動、安否確認、情報発信等のためのホスティング	○				
	情報提供サイト（sinsai.info）のホスティング	○	○	○		
	携帯メールと位置情報の蓄積・検索・提供「J!ResQ」	○	○		○	
② 被災者救援	救援情報共有システム「SAHANA」構築	○	○	○	○	○
	輸血用血液製剤の安定供給支援	○		○	○	○

用途区分	活用事例	有効性の観点				
		迅速性	拡張性	経済性	耐災性	安全性
活動の情報インフラ	被災動物救護支援サービス	○	○			
	被災者とNPOをマッチングするクラウドサービス	○	○			
	農山漁村被災者受入れ情報システム	○	○			
	震災復興支援システム	○				
③ 行政情報提供サイトの拡張	クラウド環境にミラーサイトを構築し、アクセス集中に対応	○			○	
	「東日本大震災　子どもの学び支援ポータルサイト」にクラウド型情報基盤サービスを提供	○	○			
④ 被災企業等の緊急情報発信・業務処理	アクセス急増した震災情報システムにIaaS環境で対応	○				
	被災地向け安否確認・Web会議の提供	○				
	大学連携高度教育基盤システム	○	○		○	○
	取引先企業の被災状況や工場稼働状況の確認	○	○		○	○
	サーバ、PC の重要データを保存し共有できる場所を提供				○	
	仮想デスクトップ提供	○			○	
	仮想サーバのリソースを無償で提供	○	○	○	○	○

■ 他に抽出された知見

- データセンターそのものは被害なし。しかし、ほとんどのネットワークが途絶し、データセンターを利用できなかった。ネットワークの多重化、ネットワーク途絶時に運用できる縮退運用環境の確保及びネットワーク復旧時にデータの同期を図れる仕組みが必要である。
- 停電時の運用継続のため、燃料の確保が課題として認識されていた。
- 被災した地方公共団体では、データセンター活用への移行を前向きに検討している。

3. 東日本大震災におけるデータセンターの緊急対応の実態と課題（実態調査その３）

3.1. 調査の概要

東日本大震災に際しては、被災地ならびに関東地域にあるデータセンター（DC）およびクラウドサービスにおいて、震災による直接の被害や、電力その他のユーティリティの供給制約の中で、サービスを維持するために非常時対応の対策が実施され、有効に機能した。

本節では、データセンターならびにクラウドサービスを提供している事業者を対象に、東日本大震災時の実態について調査し、緊急時に機能やサービスを維持するための要件を抽出した。

3.2. 調査の方法

東日本大震災の影響を受けたと想定される、東北・関東地域に立地するデータセンターおよびクラウドサービスを運営する事業者を 9 社選定し、インタビューを実施。インタビューが難しい事業者については、既存資料の調査を実施し、緊急時に機能やサービスを維持するための要件を抽出すべく、分析を実施した。

分析に当たっては、以下の要件が含まれていることに留意して実施した。

① 平常時におけるライフラインの冗長性確保
② 緊急・災害時における代替ライフラインの確保
③ 緊急・災害時における代替ライフライン確保のための二次的サプライの要件
④ 通信回線に関する平常時ならびに緊急時の要件
⑤ データセンターの運転ならびに保安のための要員に関する要件
⑥ 意図を持って行われるサイバー攻撃に対する防衛または回避

東日本大震災時の対応だけでなく、大震災発生前の対策、どの対策が上手く機能したか、震災時には表面化しなかったが、東日本大震災以上の震災が発生した際に表面化すると想定される課題事項についても言及する。

【インタビュー実施対象会社】

✧ 通信系事業者
- KDDI 株式会社
- 株式会社インターネットイニシアティブ
- NTT コミュニケーションズ株式会社

✧ SI 系事業者
- 富士通株式会社
- 日本 IBM 株式会社
- 日本ユニシス株式会社

・ 株式会社野村総合研究所

【既存資料調査対象会社】

・ ソフトバンク株式会社
・ Amazon Web Service(AWS)

※ ソフトバンクおよび AWS は既存資料より東日本大震災時のサービス実態のみ調査。

【主なインタビュー項目】

✧ 災害等の緊急時に対する対策状況について
  ・ ハード面における対策状況
    ✧ データセンター設備（電気・水道・ガス等のライフライン、自家発電設備など）
    ✧ クラウドサービス基盤の対策状況
  ・ ソフト面における対策状況
    ✧ 運転要員の確保状況
    ✧ 緊急対応マニュアル準備状況
    ✧ 各種データ保管状況
✧ 東日本大震災発生時における緊急対応の実態について
  ・ 震災発生直後
  ・ 震災発生後のライフライン途絶時
  ・ 震災発生より一定期間後
  ・ 震災による特殊事例発生時
  ・ 震災時における緊急対応の反省点、今後検討すべき課題
✧ クラウドサービスおよびデータセンターにおける情報セキュリティへの対応状況
✧ クラウドサービスの利用事例

3.3. 大規模災害時におけるデータセンターの対応と課題

インタビュー結果の詳細は図表 91 にまとめたが、各社の対応と明らかになった課題について、項目別に紹介する。

3.3.1. 平常時における緊急事態対応の準備状況

(1) ハード面における対策状況

① データセンター設備

データセンターのハード面における対策、「データセンターの躯体構造」、「ライフラインの確保状況」、「緊急時の仮移転準備」の 3 点の取り組みについて把握した。

データセンターの躯体構造

データセンターの躯体構造については、各事業者とも耐震構造であり、制震・免震構造(装置)を備えているものも多い。立地についても活断層の有無を事前に調査していると回答する事業者もあった。

ライフラインの確保状況

ライフラインに関しては、商用電源、非常用電源について調査を行った。商用電源に関しては各社とも冗長化を図っている。具体的な対応としては、少なくとも 2 箇所の変電所から受電している。その上で 1 変電所から 2 系統の受電を行っている例や、さらには電力会社 2 社から受電している例もあり、商用電源の冗長化については各社とも十分な取り組みがなされているとみられる。

停電時の電源については、各事業者ともUPSならびに非常用自家発電装置を備えているが、自家発電装置の燃料備蓄については、データセンターの立地条件に応じた消防法の規制やデータセンターのティア [69]等によって基準が異なっている。但し、複数の燃料供給元との優先供給契約は各社とも締結している。

緊急時の仮移転等の準備の有無

調査対象の各社とも、国内の他地域もしくは国外にデータセンターを保有しており、必要に応じて緊急時にバックアップや仮移転が可能であった。なお、国内においては、東日本と西日本にそれぞれ 1 拠点というように、距離や電力供給区域を考慮してデータセンターの配置が行われている。

② クラウドサービス基盤の対策状況

データセンター設備の上にクラウドサービス基盤が運用されるため、基本的には前項の対策状況はカバーすることになるが、クラウドサービス基盤側で行う対策として「通信回線の冗長化」およびクラウドサービスにおける事業継続計画(BCP)つまり「ディザスタリカバリー(DR)サイト」の準備が挙げられる。

通信回線については、各事業者とも異なる通信キャリアの有線回線による冗長化を図っ

[69] データセンターに求められるパフォーマンスのレベルごとに定められた施設要件の階層。ティア 1 から 4 まで規定されている。数字が大きいほど求められるサービス継続性の要件が高くなる。

ている。通信事業者系クラウドの場合でも、ユーザニーズが多いためか、自社回線＋他社回線による冗長化を図っている。また、緊急連絡用に衛星電話の設置を行っている事業者も多い。

また、調査対象の各社とも複数のデータセンターを運用しているため、そこにクラウドサービス基盤のDRサイトを構築する形態であった。ただ、DRサイトを利用するには各社とも別途オプション費用が必要になる。オプション費用を払うことで、他地域（場合により国外）のデータセンターでリカバリー可能となる。

(2) ソフト面における対策状況

ソフト面における対策として、「運転要員の確保」、「緊急対応マニュアルの準備」、「各種データ保管」の 3 点について現状の取り組みを把握した。

① 運転要員の確保状況

緊急時の運転要員については、各社とも通常のシフト要員で対応可能であるとの回答が多かった。その中で、大手通信系事業者は、緊急時に必要であればデータセンターの要員以外に通信局舎の運転要員を追加招集することが可能という回答であった。これは、データセンター、局舎を含め設備ならびに運転要員を多く所有する通信系事業者の特徴と言える。

次に、運転要員の食料と飲料水については数日分を確保しているという回答が大半を占めた。一般的に被災時に孤立した場合、最低 3 日間の食料と飲料水の備蓄が推奨されている。これは、3 日後には被災地外からの救援が届くという前提で推奨されているものであり、この観点からは問題はないものと考えられる。ただし、正確な日数については把握していないとのコメントが多かったことから、正確な備蓄数の把握が求められる。合わせて鮮度（消費期限）の管理を徹底しておくことが必要と考えられる。

② 緊急対応マニュアルの準備状況

緊急対応マニュアルについても各社とも作成済みであり、災害対応訓練も定期的に実施している。訓練の規模により間隔は異なっているものの、最短毎月、長くとも半年に 1 回程度何らかの訓練を行っている。ただし、東日本大震災時に有効に機能したマニュアルとそうでないものとが混在しており、各社見直しを実施している。

③ 各種データ保管状況

ここでは、クラウド事業者とユーザが管理するデータが混在し、管理の役割分担が複雑になるIaaSを前提に、クラウド事業者のデータ保管状況について把握した。

把握した項目は、「クラウド事業者のデータ保管対象（デフォルト）」、「クラウド事業者のデータ保管対象（ユーザ管理範囲の代行保管）」、「保管データのバックアップの有無」、「保管データ量及び増加スピード」、「保管期間」、「復旧方法」の 6 項目である。

クラウド事業者のデータ保管対象（デフォルト）

IaaS における事業者の管理範囲はホスト OS レイヤー以下にあたるが、その部分の各種運用ログ（アクセスログ、イベントログ等）およびシステムバックアップを保管対象とする回答が大半を占めた。

クラウド事業者のデータ保管対象（ユーザ管理範囲の代行保管）

IaaS におけるユーザの管理範囲はゲスト OS レイヤーより上にあたるが、クラウド事業者によっては、ユーザ管理範囲のデータについて、ユーザから委託を受けてデータバックアップを取得・保管している事業者も多くみられた。これは、今回ヒアリングしたクラウド事業者の大半が SIer を兼ねているためだと推測される。また、ユーザ管理範囲データの代行保管を実施する担当者はクラウドサービス管理者とは別組織になることが一般的であることも分った。セキュリティ・プライバシーへの配慮の現われと考えられる。

保管データのバックアップの有無

各社とも当然ながら管理範囲データについてはバックアップを取得している。バックアップデータの保管先として、遠隔地バックアップは 2 社にとどまり，大半は同一センター内の別筐体へ保管している。

保管データ量及び増加スピード

保管データ量の正確な数値はほとんど明らかにされなかったが、大半の事業者からは保管データが今後も増大していくとの見通しが示されている。

保管期間

保管期間について、「上限を設けていない」事業者から「5 年程度」の事業者に至るまで、まだ混在している状況である。

復旧方法

各社とも復旧方法として標準的なリストアによる復旧方法を採用している。

④ その他

ソフト面における対策の中で大規模災害以外に実施しているものとして、パンデミック（感染症の爆発的流行）への対応を取っている事業者も見られた。

3.3.2. 東日本大震災における対応

基本的には、今回調査対象となった事業者においてはサービス停止等の大きな影響を受けていない。また、日本データセンター協会に対するインタビューにおいても、事業としてデータセンターを運営している事業者に関しては、甚大な影響を受けたという報告はないとのことであった。

(1) 地震の検知からサービスの状況確認までの対応

地震の検知とサービス継続確認に至る対応については以下のようなものであったという。地震の感知については、オペレータからの連絡、一般的な緊急地震速報システムの他、事業者によってはNPO法人リアルタイム地震情報利用協議会 [70]から提供される高度な地震速報を活用しているケースもあった。各社とも東日本大震災時には地震の感知・検知から 10 分～1 時間程度でサービス継続の確認に至っている。

(2) ライフライン途絶への対応

ライフラインの途絶については、東日本大震災時は多くの事業者で停電を経験している。今回は各データセンターとも自動で商用電源から自家発電に切り替えを実施している。その後、データセンターの設置エリアにより差があるが、8 時間～24 時間後に商用電源が復旧した。商用電源復旧後、多くの事業者で手動手順により自家発電から商用電源への切り戻しを実施しており、切り替えについては問題は生じていない。

自家発電装置への燃料補給は、停電が長時間にわたった 3 社で実施されている。このうち 1 社では近隣の供給元からの補充調達が難しかったため、遠隔地の燃料供給元から調達せざるを得ないという問題に直面した。それでも今回は商用電源の復旧が比較的早かったため、多くの事業者では燃料補給の問題は深刻化しなかったものの、今後の燃料確保について課題であると認識している。

(3) 東日本大震災で初めて直面したリスクへの対応

東日本大震災による原子力発電所の緊急停止や事故の影響で電力の供給能力が不足し、計画停電が行われた。この計画停電の対象となった事業者もあったが、数時間程度であり、事前の対応手順に従って大きな問題なく対応が可能であった。

(4) 緊急対応の反省点と今後の課題

このように、サービスが途絶しなかった理由は、建物自体が堅牢であったこと、緊急時対応マニュアルが機能したこと、自家発電燃料供給会社との優先供給契約や複数の供給会社と契約していたことが機能したことがあげられる。しかしながら、半数以上の事業者からは「自家発電燃料が切れた場合の対応方法」を課題として挙げられた。これは、今回の東日本大震災以上の災害が発生し、商用電源停止時間がさらに長時間になった場合に、現在の備蓄量や優先供給契約だけでは対応が困難になると多くの事業者は考えているため

[70] 同協議会の Web サイト http://www.real-time.jp/

である。

たとえば、燃料優先供給契約を結んでいたにもかかわらず、実際には供給が滞り、代替供給元の探索と実際の補充調達に時間がかかった事例が見られたことから、優先供給契約だけでは安全とは言い切れないという認識がある。また、日本データセンター協会も「非常用発電機の燃料確保」を東日本大震災における最大の教訓に挙げ、燃料調達先の複数化（可能であれば異なる石油元売り）を推奨し、加えてデータセンターのファシリティ基準のうち自家発電装置の燃料確保量について、優先供給契約によって確保した分を除外する変更を行った[71]。

ただし、コストはもとより、設備面の制約や消防法の規制により無限に備蓄量を増やすことはできない。このため、技術的にはデータセンターの消費電力を抑えることと、自家発電装置の燃料効率を高めることが望まれる。具体的には、冷却効率の改善、省電力 IT 機器の適用などのエネルギー効率化ソリューションや、石油以外の代替エネルギーを活用したソリューションなどが出てきているため、各データセンターの置かれている状況に合わせ、このようなソリューションを検討していく必要がある。一方で、燃料供給の優先順位を高められるよう、社会的なコンセンサスを得ていくことも求められよう。

また、事業者とのヒアリングでは出てこなかったが、燃料だけでなく、運用者向けの水・食料の確保も同様と考えられる。一般的な備蓄量としては、1 人あたり 3 日分と言われている。データセンター事業者へのヒアリングでは数日～10 日分という回答が大半であったため一般的な水準はクリアしている。しかし、仮に備蓄量を超えて水・食料が必要になった場合を考えると、近隣の自治体との協力が考えられる。各自治体で非常食を備蓄しているため、有事の際にどうするか事前に協議する必要がある。

(5) 震災の経験を踏まえた今後の対応

各社とも上述したように自家発電用燃料の確保について課題を感じている。また、発災時の社員との連絡等の通信手段の確保についても、今後見直しを進めるとしている事業者もある。さらに、今回の経験を踏まえ、マニュアルや訓練の見直しを計画している事業者もあった。

また、データセンターの被害はなかったものの、沿岸部埋め立て地等での地盤液状化とそれによる建造物ならびにライフラインの被害が報告されており、立地選定やデータセンターの躯体の設計においては今後考慮することが必要となると考えられる。

3.3.3. クラウドサービスのセキュリティ対策について

セキュリティ対策については、以下の項目について把握した。

- OS やアプリケーション等のシステムに関するセキュリティ対策
- データ管理対策

[71] 日本データセンター協会「東日本大震災を踏まえたデータセンター　ファシリティ スタンダードの検証と見直し（ダイジェスト版）

・ ネットワークと通信に関するセキュリティ対策
・ 物理的アクセス管理に関するセキュリティ対策
・ 運用要員に関するセキュリティ対策

(1) システムおよびデータ管理におけるセキュリティ対策

各社とも、多少の差異はあるものの同様の対策ができている。システムそのもののアップデートによるセキュリティ向上は事業者の管理範囲では適切なタイミングで行っている。また、ユーザ管理範囲のシステムについては、基本的にユーザ判断となるが、事業者からの情報提供を行ったり、サービスとして受託して実施したりする例がある。

また、事業者管理部分のハードウェア(サーバ、ストレージ、ネットワーク)については各社とも冗長化を実施している。

データ管理に関するセキュリティ対策について、サイバー攻撃対策の考え方で、攻撃を防御する対策と仮にデータが盗まれたとしても改ざん・漏えいまでには至らないようにする対策がある中で、後者の対策としてストレージ暗号化メニューを提供するクラウド事業者が数社あった。

(2) ネットワークと通信に関するセキュリティ対策

ファイアウォール、IPS[72]やIDS[73]による不正侵入防止、検知、遮断は各社とも実施しているほか、ウィルスチェックソフトの提供、アップデートなども行っている。サイバー攻撃に対する監視、検知、解析についてもオプションとして提供している事業者が多い。

特徴のある取り組みの一つとして、あるゲストバーチャルマシンで通信中のパケットに不審な挙動が発見された場合、当該ゲストバーチャルマシンを停止して他のユーザの保護を図ることを選択肢に入れている事業者がある。

(3) 物理的アクセス管理に関するセキュリティ対策

物理的アクセス管理については、入退館管理等のデータセンター施設に対するもの、およびデータセンター内においてクラウド基盤を構成する各機器(サーバ、ストレージ、ネットワーク等)に対するものの 2 点について把握した。

まず、データセンター施設へのアクセス管理については、入退館管理、持ち出し管理などは当然実施されており本人認証のための生体認証設備や、持ち出し管理のためのスキャニング装置などの高度な設備を設置している事業者もある。

機器に対するアクセス管理については、ラックの施錠管理、各機器のログインID・パスワード設定などの対策を各事業者とも実施している。

(4) 運用要員に関するセキュリティ対策

直接的なセキュリティ対策ではないが、運用要員に対する情報倫理・非行対策について、

---

72 Intrusion Prevention System:不正侵入を検知した場合に通信を遮断する装置

73 Intrusion Detection System:不正侵入検知装置

「身元・履歴確認」、「服務規律・就業倫理教育」、「システムとデータへのアクセス権・特権管理」の 3 点を調査した。

身元・履歴確認について、各社とも自社もしくはグループ会社で運用要員を採用する際は、身元・履歴確認を実施している。また、運用要員を外部委託している事業者では、契約で担保するようにしている。

服務規律・就業倫理教育は各社とも自社で策定したポリシーに則り、運用業務におけるルールや情報倫理に関する教育を実施している。

また、システムとデータへのアクセス権・特権管理について、運用要員と管理者などの役割の違いによりアクセス権限や管理者特権を設け、役割以外のシステムを操作できないようにしている。

これらの対策が有効に働いているか確認するために、運転要員の作業や業務に関するモニタリングを行っている。具体的には、操作ログを取得したり、モニター越しに管理者が運用要員の監視を実施している。また事業者によっては内部監査なども行って、万全を期している。

(5) セキュリティに関する情報開示

セキュリティマネジメントという観点でセキュリティに関する情報開示についてのヒアリングも実施したので、参考までに記載する。大きく 2 つの観点があり、一定の基準を満たしていることを外部に示すために事業者が取得した第三者認証を開示するものと、利用者側の監査等で必要な場合に実際の取り組み内容を開示するものがある。各社とも両方の開示を実施していた。ヒアリングの際に出てきた主な第三者認証は、一般財団法人日本情報経済社会推進協会（JIPDEC）が認定する情報セキュリティマネジメントシステム適合性評価制度（ISMS）やプライバシーマーク、AWSが取得したことで話題になった、クレジット業界におけるグローバルセキュリティ基準であるPCI[74]データセキュリティスタンダード（PCI DSS）などがある。

(6) セキュリティに関する今後の課題

これまで見てきたとおり、各社とも必要と考えられるセキュリティ対策を実施しており、現状の対策でセキュリティインシデントの発生というようなトラブルに関する話はなかった。ただし、質的に改善させるという意味合いで、「ハイパーバイザーレイヤーの脆弱性対策の改善」、「データセンターへの機器持込持出管理の改善」を今後の課題として挙げている事業者があった。

74 Payment Card Industry

図表 92 各事業者のインタビュー結果

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
震災の影響範囲にあったクラウド基盤もしくはDC の所在地			・震災影響を受けたクラウド基盤、DC なし。 ※クラウド基盤があるDC は3箇所（関東、関西、北海道）	・震災に関する項目については、東北地方に所在する DC を対象に回答する。 ※クラウド基盤があるDC は関西と中国の2箇所	・震災に関する項目については、東北地方に所在する DC を対象に回答する ※クラウド基盤があるDCは東日本と西日本の2箇所	・震災に関する項目については、東北地方に所在するDCを対象に回答する。 ※クラウド基盤があるDC は関東と関西の2箇所	・震災に関する項目については、関東地方に所在するDCを対象に回答する。 ※同所にあるクラウド基盤は震災後にサービス開始	・震災に関する項目については、東北エリアのDCを対象に回答する。 ※クラウド基盤があるDCは東日本と西日本に展開	・関東地方にあるDCにクラウドサービスを展開しており、計画停電の対象となっており、そのDCに関して回答する。
クラウド・DC サービスにおける緊急時の対策状況	DC 設備	ライフライン冗長化の有無	・電力のみ冗長化 ※2箇所の変電所から電力供給	・電力のみ冗長化	・電力のみ冗長化	・電力のみ冗長化 ※電力会社2社から引込み	・電力のみ冗長化	・電力のみ冗長化	・電力のみ冗長化 ※2 箇所の変電所から 2 系統＋1系統の計3系統を引込み
		無停電設備設置の有無	・各事業者とも「UPS、自家発電有り」						
		自家発電設備燃料の備蓄状況と補充する際の条件	・72 時間分備蓄 ・複数の燃料供給会社と優先契約	・DC により 24 時間もしくは 48 時間分備蓄 ・残量が 50%切った場合に補充 ・複数の燃料供給会社と優先契約	・DC により 24 時間もしくは 48 時間分備蓄 ・自家発電稼働する度に補充している。 ・複数の燃料供給会社と優先契約	・DCにより48時間もしくは 72 時間分備蓄 ・自家発電稼働する度に補充している。 ・複数の燃料供給会社と優先契約	・社内基準にもとづき数日分備蓄。 ・補充条件も社内基準にもとづき補充している。 ・複数の燃料供給会社と優先契約	・DC により24、48、72 時間分備蓄 ・自家発電稼働する度に補充している。 ・複数の燃料供給会社と優先契約 ・電源車を所有している。	・自家発電設備燃料について、消防法上で定められている範囲内で備蓄している。 ・社内基準にもとづき補充している。 ・複数の燃料供給会社と優先契約
		緊急時に仮移転等の準備の有無	・東京・関西・北海道の DC にてマルチ運用（オプション）が可能。	・他地域 DC にて DR 可能 ※オプション	・DR についてはファイルサーバサービスのみ ・他サービスはバックアップとって、サイト復旧時にサービス復旧となる。	・他地域のDCへ移行を計画 ※グループ内のDC 間でリングを組むなど ・コンテナタイプの DC も今後作る予定。	・国内含め全世界に 6 拠点がある。	・他地域の DC にて DR が可能 ※クラウドサービスとしてはオプション	・他地域（関西）の DC にて DR が可能 ※オプション
	通信回線	DC 側回線冗長化の有無	各事業者とも「異キャリアによる冗長化」						
		回線冗長化の組合せ	各事業者とも「有線による多重化」						
		DR サイトの有無	各事業者とも「オプションで DR 対応可能」						
	保守要員	緊急時に追加要員招集するか	・追加要員はない。 ・通常のシフト要員で運用	・追加要員はない。 ・通常のシフト要員で運用	・追加招集あり。 ※緊急時は他地域の局	・追加要員はない。 ・通常のシフト要員で運	・追加要員はない。 ・通常のシフト要員で運	・状況により、追加招集する。	・計画停電時やセンター単体の緊急時は別途要因招集

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
					舎、センターから追加召集	用 ※当該 DC には要員が 200 名いる	用 ・状況により、マネージャーについては追加招集する。	※計画停電時に念のため招集した	する想定でいるが、昨年の東日本大震災規模の場合だと、追加招集は現実的でないと考えている。
		緊急時の食料備蓄状況	・1 人当たり 7 日分の乾パンを備蓄 ※震災前は 3 日分だった	・1 人当たり約 10 日分の食料を備蓄	・数日分の食糧備蓄有り	・数日分の食糧備蓄有り	・数日分の食糧備蓄有り	・正確に把握してないが、数日分の食糧備蓄有り	・数日分の食糧備蓄有り ※食料・飲料の備蓄は 120～130 食分ある。
	緊急対応マニュアル	震災前準備の有無	・震災前にマニュアル準備済み	・震災前に以下準備済み ※災害対応フロー、緊急対応マニュアル、安否確認システムなど	・震災前に以下準備済み ※全体フロー、安否確認システム、初期損害チェックリスト。	・震災前にマニュアル準備済み。	・震災前にマニュアル準備済み。	・震災前にマニュアル準備済み。 ※大規模障害時のノウハウは溜まっており、それを元にしたマニュアルがある。	・震災前に以下準備済み。 ※安否確認システム、地震発生時の確認リスト。 ・コンピュータ稼働のために以下の対策を実施。 ・電源冗長化 ・発電機のクラスタ化 ・UPS、空調機、冷凍機の予備 →損害レベル別に4段階に分け。LV4 になるとコンピュータに影響あり
		災害訓練の有無	・安否確認テストを 2 カ月に1回実施。	・災害訓練は、定常的（半年に1回）に実施している。	・災害訓練は、定常的（月1回）に実施している。 ※震災前は3カ月に1回	・災害訓練は、定常的（月1回）に実施している。	・災害訓練は、定常的（月1回）に実施している。	・災害訓練は、定常的（年数回）に実施している。 ※会社として大規模障害時想定した対策本部、エスカレーションの安否確認は年に数回、大規模障害を想定した災対フロー訓練も実施。	・災害訓練は、定常的（週1回）に実施している。 ※毎回被害個所を変えて、訓練実施。
	各種データ保管	データ保管対象 （事業者範囲） ※デフォルト	・ホスト OS レイヤーのシステムバックアップ、各種運用ログが対象	・ホスト OS レイヤーのシステムバックアップ、各種運用ログが対象	・・データの保管対象は、ファイルサーバの DR オプション契約分 ・各種運用に必要なログ（監視ログ、アクセスロ	・ホスト OS レイヤーのシステムバックアップ、各種運用ログ、課金データが対象 ・ゲスト OS 以上のレイヤ	・当社管理部分並びにユーザ作成分も含めた VM のイメージをバックアップしている。	-	・ホスト OS レイヤーの各種運用ログが対象

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
					グ） ・仮想サーバのスナップショット（IaaS,PaaS 系以外）。	ーが対象でユーザにてバックアップ			
		データ保管対象（ユーザ管理範囲の代行保管） ※オプション	・ゲスト OS 以上のレイヤーの各データ	・ゲスト OS 以上のレイヤーの各データ	・代行取得しない	・代行取得しない	・ユーザ管理の DB	・ゲスト OS 以上のレイヤーの各データ	・ゲスト OS 以上のレイヤーの各データ
		保管データバックアップの有無	・北海道 DC に遠隔地バックアップ	・遠隔地バックアップ	・ファイルサーバの DR オプション契約分については DR サイトへバックアップ（遠隔地バックアップ）。 ・その他データについては、同一センター内の裏サーバへ Disk to Disk でバックアップ。	・別筐体への DisktoDisk によるバックアップ。	・ユーザバックアップ分については、別筐体に Disk to Disk でバックアップ ・自社管理分については、外部媒体へバックアップしている。	・ユーザ指定で Disk2Disk、テープ、遠隔地バックアップが可能。	・データバックアップについて、同サイト内に保管。 ・今後遠隔地バックアップ予定
		保管データ量及び増加スピードについて	・回答差し控え	・保管データは数ペタバイトのレベル。スピード感としては年ごとに倍増。	・保管データ量については開示できないが、増加スピードは、昨年から1年間で 6 倍増えている。	・ビッグデータソリューションの引き合いもあり、データ量はかなりある。テラバイトクラス。	・保管しているデータ量および増加スピードについては、クラウドサービス全体では数ペタバイト、当該DCだけでも数百テラバイトが利用されている。	・回答差し控え	・回答差し控え
		保管期間	・回答差し控え	・データ保管期間の制限は現状設けていない。	・データ保管期間について、ファイルサーバの DR オプション契約分はユーザ契約期間まで。運用ログの保管期間は定めていない。VM のスナップショットは 1 世代分。	・明確に決まってないが、大体 5 年間。	・回答差し控え	・オプションにて、ユーザ指定可能	・ユーザデータ分は契約期間中ずっと保管。事業者側の構成情報について、サービス提供中は保管し、世代管理を実施。
		復旧方法	・NW 越しにバックアップデータ送信し、リストア	・データ復旧はリストア	・データ復旧はリストア	・データ復旧はリストア	・事業者管理データの復旧方法については、回答差し控え ・ユーザ管理範囲のゲス	・データ復旧はリストア	・データ復旧方法について、ユーザデータ分はユーザがリストアできるように API、画面を提供。事業者分はリスト

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
							トVMのデータのバックアップとリカバリーはユーザ責任で行う必要があり、そのための手段として専用ソフトを提供		アにて復旧。
	その他		・鳥インフルエンザ等のパンデミック対策としての訓練も実施	・特になし	・衛星携帯電話を各データセンター、各局舎に配備	・DC 敷地内に衛星アンテナがあり、衛星電話等の衛星を利用した通信手段を準備。	・毒性の強弱問わず、パンデミック対応を実施。非接触型の体温計などの準備物を整え、被害想定を要員の稼働率に設定し、稼働率に応じた対策を講じている。	・衛星電話を準備している。	・衛星電話を準備している。
東日本大震災時の対応状況	震災発生前	災害発生探知システムの仕組み	・影響を受けたDCはなかったため、割愛	・中央監視装置で監視を実施。オペレータからの連絡により検知。	・リアルタイム地震情報利用協議会から通知されるようになっている。これは全国の震度計を元にしており、一般的な地震速報よりも速くて確実。	・地震検知システムにて検知できるようになっている。	・震度計	・電源等各装置のアラームは24時間365日監視しており、データセンター設備の異常はそこで検知できる。	・地震感知器あり。また、LV4の災害については中央監視で検知。
		災害発生を予防する仕組み（免震構造等）		・DC の構造について、東北地方の DC は制震構造。他センターは免震構造、耐震構造あり。 ・DC 建設時に立地条件を設けている。 ※ハザードマップ上災害が少ないところ、活断層がないところなど。	・DC の構造について、DC によって様々だが、東北地方の DC は耐震構造。	・当該 DC は免震構造	・当該DCのラックのあるフロアについては床面免震、それ以外は全社共通の耐震構造。	・DC の耐震構造は、ビルによって様々。最近は免震構造が多い。 ・当該 DC は耐震構造。	・DC の構造については免震構造。 ・立地について、活断層がないなどの調査を実施。官公庁1類基準に合わせる形で梁の太さや鉄骨の筋かいを用いている。
	震災発生時	災害探知してからサービス継続確認に至るまでの対応（時系列含め）		・検知から確認までで約10分程度。 ※地震発生→NW 監視で全断検知→停電→非常用電話で自家発電切り替えを確認。	・当該 DC は通信の基地局も兼ねていたので、確認に多少時間がかかった。 ・※地震発生→揺れを検知→停電→自家発電に自動切替→サービス継	・・時系列は現場担当が詳しいが、利用者への第一報（影響の有無のみを連絡）は 30 分以内にできていた。 ※確認項目	・検知から確認までで約1時間程度。 ・並行して対策本部設置（発生から数時間後） ・海外 DC を利用して日本のお客様のミラーサ	・クラウドサービスは監視システムでアラーム監視している。クラウドサービスではお客様システムに影響のあるにアラームは無かったと聞いている。 ・コロケーションサービスと	・検知から確認までで約 30 分程度。 ・ ※時系列 ・停電発生し、自家発電切替確認まで約 6 分 ・中央監視モニターで停電等

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
					続確認（各ラックへの巡回確認含む）。	・管制塔にてセンター内の共用設備（NW 等）に異常ないか確認 ・温度、空調管理システムにて異常ないか確認 ・ラックや大型機器等の床置き機器に影響ないか巡回して確認	イトを立ち上げるなどの支援を実施。	して、当該 DC は自家発電エンジンを監視していて、震災の影響を確認。	の目視確認完了：約15分 ・各マシン室に巡回しラック状況の確認：約30分
	震災発生後のライフライン途絶時	発生直後のライフライン断絶時（停電等）の対応（どの程度の期間か、有人/無人など）		・有人にて対応。自家発電に自動切替、自家発電で 21 時間稼働後、商用電源が復旧し、手動で切り戻し。商用電源復旧前に1回燃料補給を実施。 ・また、オペレータ自身の住居等も被災し、家族の安否確認や周辺の交通機関がマヒするなどの事情もあり、2 日後に福岡からの遠隔運用に切替。（福岡から遠隔で入退館管理を実施）	・有人で対応。自家発電に自動切替、自家発電で約 24 時間稼働後、商用電源が復旧し、手動で切り戻し。 ・燃料補充について、燃料確保が一般的に困難だった状況から、燃料を金沢の燃料供給先から補充してもらった。震災の影響で近辺の供給先よりも金沢が一番速かったため。	・有人にて対応。停電後、UPS/自家発電に自動切替、約8時間経過後、商用電源復旧し、手動戻し実施。	・有人にて対応。停電後、UPS/自家発電に自動切替、商用電源復旧し、手動戻し実施。	・有人にて対応。震災時は、自家発電燃料の有無、給油調達確認など電話会議などを駆使して現地と対応。 ・自家発電は自動切り替え、巡回確認はオペレーションで実施。	・有人にて対応。停電後、UPS/自家発電に自動切替、商用電源復旧し、手動戻し実施。
	震災発生より一定期間後	震災発生直後の対応策に時間的制約があった場合、その制限を迎えてからシステムはどう対処しましたか（自家発電の燃料切れ等）		・震災時は時間的制約（燃料切れ）を迎える前に商用電源が復旧した					
		システムが万が一停止してしまった場合、どう対処していましたが（システムの復旧にかかる期間）		・仮に燃料が切れた場合は、どう対処すればいいか、課題となっている。	・仮に燃料が切れた場合は、どう対処すればいいか、課題となっている。	・現在はシステム停止後どうするかよりも停止しないようにどうするかを検討している。自家発電燃料を切らさずに、燃料補給のシミュレーションを綿密に練って	・現在はシステムが万が一停止する事態までは想定していない。それよりもいかに燃料補給を切らさないようにするかを検討している。	・万が一、発電機の燃料供給などが間に合わなくなり、電源断の予定がでた場合は、ユーザ周知とともにサーバシャットダウンして DR へ切り替えることが考えられる。	・現在はシステムが万が一停止する事態までは想定していない。それよりもいかに燃料補給を切らさないようにするかを検討している。

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
						いる。			
	震災による特殊事例発生	計画停電等の特殊事例が震災発生から数ヶ月経過しても続いた際、事業者としてどのように対応したか。		・関東地方所在の DC が計画停電対象になり、2回実施されたが、想定通り、自動で自家発電切り替え、計画停電終了後手動切り戻しを実施。	・3 回ほど計画停電の対象となった DC があったが、想定通り自家発電への切替による対応を実施	・1，2回計画停電の対象になったが、自家発電への切替対応で問題なくサービス維持している。	・当該 DC は計画停電による影響は発生していない。	・計画停電対応は、自家発電へ切り替え、プロセスに沿って確認、商用電源に戻してからは燃料補給を実施。 ・一部ユーザからは補給のタイミングや残運転時間を教えてほしいという要望あり	・計画停電の対象に2回ほど該当したが、想定プロセスに従って対応。
		結果どのようにサービスは維持されたか		・サービス影響なし					
	緊急対応の反省点、今後の課題			・自家発電用燃料が切れた場合の対応方法が課題。 ・燃料供給先は複数契約しているが、大規模災害で道路寸断など物理的に燃料運搬が難しい状況になった場合にどうするかが課題。 ・備蓄を増やすという選択肢もあるが、特にビル型 DC では備蓄量を増やすことができず、課題としている。 ・2 点目に電力会社から優先的に情報を入手できるようなパスがないことが課題としてある。	・自家発電用燃料が切れた場合の対応方法が課題。 ・自家発電用の燃料の問題がある。停電が長引いた場合を考えると、緊急時の燃料供給先を増やさないといけないと考え、複数の業者からの供給体制を整備した。（備蓄量を増やすことは建築基準法に抵触することもあり、時間がかかるため、対策としては現実的ではない）	・自家発電用燃料が切れた場合の対応方法が課題。 ・そのために、燃料補給をどのタイミングで実施するかのシミュレーションを綿密に練っている。	・震災時に安否リスト確認で確認が取れない社員がおり、その場合どうすべきか課題となっている。 ・ネットワーク断絶時に、衛星電話設備の設置など、連絡系どうするか課題となっている。	・震災時対応や計画停電時対応は想定よりもスムーズに対応できており、今のところ課題は少ないと思っている。	・燃料優先供給契約先の拡大 ・マニュアル類、訓練方法の見直し。全体フローにおける優先順位の見直してもっと効率いいやり方を模索している。（震災時は中央監視のアラームが大量に出て判別するのに時間かかった）
クラウドサービスにおけるセキュリティ対応	システムに関する対策	OS やアプリケーションのアップデート、セキュリティ修正パッチやサービスパックの適時適用等	・ユーザ要望に応じて OS のセキュリティ修正パッチやサービスパック適用を実施 ・アプリについては、機能	・事業者管理範囲（ホスト OS）については、サービス影響与えないように、クリティカルなもののみ事前検証した上でセキュ	・事業者管理範囲（ホスト OS）については、毎月のメンテナンス時間に随時実施。緊急性の高いパッチは緊急借用をとっ	・事業者管理範囲（ホスト OS）は適時適用している。 ※IaaS はホスト OS、SaaS の場合はアプリ	・事業者管理範囲（ホスト OS）は、社内セキュリティ基準に従い、重要度に応じて修正パッチ、サービスパックを適	・事業者管理範囲（ホスト OS）は、クリティカル度が高いパッチは検証の上、事業者側で実施。 ・ユーザ管理範囲（ゲスト	・事業者管理範囲（ホスト OS）は、サービス影響与えないように、クリティカルなもののみ事前検証した上でセキュリティパッチを適用して

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
			追加等で随時対応	リティパッチを適用している。 ・ユーザ管理範囲（ゲストOS 以上）はユーザ判断。 ※なお、ユーザ管理範囲のセキュリティ対策を個別SIとして受託することがある。	て、実施している。	ケーション部分まで	用している。 ・ユーザ管理部分（ゲストOS以上）はユーザにて対策。	OS 以上）はユーザにて対策。事業者としては、パッチ情報の連絡のみ。	いる。 ・ユーザ管理範囲（ゲスト OS 以上）はユーザにて対策。クリティカルなパッチで、把握している分はユーザに通知している。
		システムの可用性・信頼性を確保するための対策 ※事業者範囲分	・サーバ、ストレージ、NWの冗長化実施。 ※物理サーバの冗長化はオプション	・サーバ、ストレージ、ネットワークの冗長化実施。	・サーバ、ストレージ、ネットワークの冗長化実施。	・サーバ、ストレージ、ネットワークの冗長化実施。	・サーバ、ストレージ、ネットワークの冗長化実施。	・サーバ、ストレージ、ネットワークの冗長化実施。 ※サーバ、ストレージ冗長化はオプション	・サーバ、ストレージ、ネットワークの冗長化実施。
	データ管理対策	ストレージ暗号化の自動実施、または暗号化機能の提供	・データ暗号化サービス（センター内秘密分散／センター外秘密分散）を提供	・秘密分散サービスメニュー提供	・暗号化メニュー未提供	・ストレージは自社分、ユーザ分問わず全て自動で暗号化実施	・セキュリティ上の理由から、一度プロビジョニングされた後のゲストVMの内容にアクセスしないことを「ノータッチ・ポリシー」として定めている。	・データ暗号化サービスは事業者として提供していない。	・グループ会社に暗号化ソリューション（シークレットシェア（秘密分散））があり、要望あれば紹介している。
	NWと通信に関するセキュリティ対策	ウイルス・マルウェア感染への対策、不正アクセスへの対策、ネットワーク障害対策 等	・オプションとして、IPS・IDS サービスおよびセキュリティ監視サービスを提供。 ・タグ VLAN によるテナント間分離を実施。	・メール含め、GW、FW、IPS/IDS により対策済み。セキュリティ攻撃に対する監視、検知、解析、報告も実施済み	・ウィルスチェック等のバンドルタイプをデフォルトで提供。 ・IaaSもFW、IPS機能をオプションで提供。また、セキュリティ攻撃に対する監視、検知、解析、報告も実施済み	・ウイルス・マルウェア感染への対策、不正アクセスへの対策、ネットワーク障害対策については、対策済み。 ・VM はデフォルトでウィルスソフト提供。またマルウェア、不正アクセス等については IDS で対策済み。これも利用者にデフォルト提供。 ・セキュリティ攻撃に監視、検知、解析、防御対策も実施済み。	・FW、IPS/IDS 等にて対応実施している。 ・ゲストVMに出入りするパケットに不審な挙動がある場合、ユーザ保護のために当該ゲストVMを停止することがある。 ・セキュリティ攻撃に監視、検知、解析、防御対策も実施済み。	・ウィルスチェック、FW、IPS/IDS を提供。デフォルトでの提供は FW のみ。依頼にもとづいて設定作業実施。FW は仮想 FW で提供し、自由度は高い。 ・セキュリティインシデントに関する監視、検知、解析、対策については、セキュリティオプションとして提供。社内のセキュリティオペレーションセンターと連携して提供している。デフォルトは防	・デフォルトで FW、オプションで IPS/IDS、監査証跡サーバサービスを提供、ユーザでウィルスファイル購入条件で、ウィルスパターンファイルの配布は事業者側で提供可能。 ・セキュリティ攻撃に対する監視、検知、解析についてはオプションにて対応。
		障害や攻撃に対する監視、検知、解析、防御対策等							

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
								御。	
	機器装置に関する対策	装置の保守、各種ケーブル（通信、電源）が傍受又は損傷から保護されているか。	保護済み						
	DC 設備に関する対策	入退館申請管理、持込・持出物管理、外部からの侵入への対策、セキュリティ区域内作業におけるルール策定等の環境的なセキュリティ対策（※1）	・※1 に記載されている対策を実施。 ・その他、手の形（掌形）による本人認証を実施。	・入口は一か所で、入退館管理は実施済み。 ・持込・持出物管理について大型機器の管理はできているが、PC やメモリについては一部管理できていないところがある。	・※1 に記載されている対策を実施。 ・当社のクラウドは通信局舎内にある特性からエンドユーザが入れないようになっている。	・※1 に記載されている対策を実施。	・※1 に記載されている対策を実施。	・※1 に記載されている対策を実施。	・※1 に記載されている対策を実施。 ・持込・持出物管理については、3D ボディチェックで実施済み。 ・維持管理者がクラウド基盤へアクセスする際の端末室について、施錠等による入退館管理ができている。
	DC 運用に関する対策	監視運用体制、運転要員の信頼性確認、勤務状況・作業内容のモニタリング等	・運転要員にセキュリティ教育実施。 ・運転要員はグループ会社の人間のみで構成。 ・物理的に運用ルームを分けている。	・運転要員の採用時確認するのと採用後のセキュリティ教育を実施している。 ・運転要員はグループ会社の人間のみで構成。 ・運用マネージャーがモニターで運転要員を監視している。	・運転要員にセキュリティ教育実施。 ・運転要員は社員。 ・アクセスログ、作業ログのチェック実施。	・運転要員は採用する際に資質調査を実施し、随時教育を実施している。 ・要員については、主に本社の人間（一部グループ会社）。 ・管理ルームが3つ（管制室、システム監視ルーム、災害対策ルーム）あるが、全てモニタリングできるようになっている。	・運転要員は外部へ委託しているが、会社間の契約事項により信頼性担保している。また、運転要員へのセキュリティ教育も実施している。	・ISMS の範囲内で運用者に教育を実施。	・運転要員は外部へ委託しているが、会社間の契約事項により信頼性担保しており、また運転要員のセキュリティ教育を実施している。 ・運転要員の勤務状況・作業内容については、社員である運用マネージャーが管理。
		システムへのアクセス権限や管理者特権の管理、操作ログの管理等	－	－	・アクセス権限や管理者特権の管理、操作ログの管理を実施。	・システムへのアクセス権限や管理者特権の管理、操作ログの管理等も対策済み。管理者とオペレータで権限を分けている。操作ログも管理している。	・システムへのアクセス権限や管理者特権の管理、操作ログの管理については、全て実施している。また、厳しい社内セキュリティ基準に則った内部監査（Audit）を実施してい	－	・システムへのアクセス権限や管理者特権の管理、操作ログの管理については、監査証跡サーバにて対応。権限も分けている（維持管理者とオペレータで分けている、オペレータは本番アクセスできない）

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
							る。		
	セキュリティ対策に関する情報開示の有無		・ISMS 取得等、情報開示実施している。特に関係省庁に対して実施済み。	・質問されれば、機密に触れない程度でできる範囲で開示している。 ・また、セキュリティレポート(年1、2回)発行し、トレンド発信や啓発活動を実施	・ISMS 取得。また、問い合わせについて、管理項目レベルでは開示する。	・情報セキュリティ格付け「AAAis」やPマーク取得	・ISO27000 台を取得し、第三者からの監査を実施している。また、ユーザ側監査で必要に応じて情報開示を実施している。	・ISMS 取得含め第三者認証を取得。また、個別の問い合わせについてもできる範囲での開示を実施。18 号対応も行っている。	・P マーク取得。また、質問されれば、機密に触れない程度でできる範囲で開示している。 ・今後、FISC 対応、ISO27000 台、PCIDSS を取得する活動始める予定。
	今後検討、改善すべきと感じた課題		・セキュリティサービス未利用者の振る舞いを抑える(踏み台対策等)ために、利用者によってはコスト増になるかもしれないが、半分標準化を検討している。	・持込・持出物管理について大型機器の管理はできているが、PC やメモリについては一部管理できていないところがあるのが課題。これは全面管理するようにしている。	・FW・IPS については、ラインナップ強化により、ユーザの選択肢を増やしてもいいのではと、考えている。また、秘密分散などの暗号化サービスを今後提供していきたいと考えている。IaaS、PaaS についてはデフォルトで自動バックアップも検討している。	・現時点では特にないが、強いて言うなら、DDoS 攻撃等のセキュリティアタック発生時に、IDS/IPS で防御しているが、ユーザへの報告をもう少しわかりやすく、きめ細やかにしていくことが一つ課題としてある。	・レガシーシステムとの融合など、今後の環境変化に応じたセキュリティ対策を講じていく必要があると感じている。	・ハイパーバイザーの脆弱性対策含めた仮想サーバ環境向けのセキュリティ対策を今後検討していく。	・第三者認証の取得が課題と感じている。
クラウドサービス内容について	顧客からクラウド事業者として何を求められていると感じているか		・利用前は、廉価型、利用型というのを求めて来るが、利用後は、継続性、安定性を求めて来る。 ※継続性はクラウド事業継続性も含めて。	・まずはコスト。我々の競合はユーザのオンプレミス環境ないし、ユーザ自社クラウド環境。国内のIT 市場全体が今度右肩上がりではなく横ばいになっていく中で、ファシリティマネジメント、アセットを持たないでいいところ、ネットワークメニューの柔軟性の3点が求められているし、提供できているところが強みとなっている。	・大企業:システム全てをクラウドに任せるとまではいかないが、70%程度をクラウドに預け、またクラウドにつながる NW 部分も含め当社に任せても安心であるように求められている。 ・中小企業:クラウドだけでなく周辺の携帯、NW 部分含め、当社がユーザ企業の情報システム部のようにカバーできることを求められている。	・柔軟性(利用形態、オンプレミスとの連携など)と高信頼性(安定稼働)	・クラウド専業ではなく、企業ユースに応じ、クラウドとオンプレミスのポートフォリオが可能であることを求められていると感じている。	・コスト削減が求められ、一方では、アウトソースに必要な高信頼性、オンプレミス並みの高品質が求められている。それぞれの要望に応えるべく、パブリッククラウド・プライベートクラウドという形でメニューを提供し、対応している。	・安価かつ高信頼、高付加価値なクラウドサービスを求められている。
	クラウドサービスで強みとしている部分		・ベンダロックインがなく、ハウジングのイメージで	・上記の通り	・NW 部分が強み。SI の方向性よりは、回線、携	・高信頼性(SLA の稼働率 99.99%)	・オンプレミスとクラウドのハイブリッド利用が	・通信キャリアとしてのクラウドを強みとしている。海	・既存のオンプレミスからのマイグレーションがしやすいよ

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
			提供できる。 ・具体的には、既存のオンプレミスからのマイグレーションがしやすいように、多くの選択肢を準備している。そこがSIerである当社が提供するクラウドの強み。		帯・スマホなどのNWレイヤーを海外含め幅広く提供できるところが強み。	・ オンデマンド性（アジリティと利用時間に応じた課金体系） ・セルフサービス（利用者がWebブラウザ上でシステム配備、運用、保守まで実施可能。システム稼働状況もダッシュボードで表示） ・ 設計の簡易化（クラウド側でテンプレート用意）	可能なところが強み。	外にあるDC基盤、通信基盤含め、ネットワークとクラウドを融合させたメニューが強み。たとえば、クラウド利用者にはセンター側のVPN回線は無料で提供するなど。運用についても、回線・クラウドのオペレーションを融合することで、強みが発揮できる。	うなソリューション提供であったり、新規システム構築に対して当社がPaaSの標準PFを提供し、アジリティ、全体のコスト最適化が図れる部分が強み。これにより、従来の基盤コストの3～4割削減が図れる。
クラウドサービス事業におけるメリットとリスク	メリット	クラウドサービス事業者が考えるクラウド利用のメリット（コスト、運用性、可用性等）	・ベンダロックインがない。ハウジングのイメージ。クラウド利用において、新たに勉強する必要がない。	-	・スモールスタート可能、拡張性あり、運用負荷軽減、仮想化技術を自社で取り込む際の工数が軽減できる、自社で購入するよりはシステム化が速い。	・2点ある。「柔軟に利用できる」と「スケールメリットを生かし、安価に利用できる」の2つ。前者はシステム稼働のピーク時、ピーク外に合わせて規模を増減できる形態であったり、スモールスタートやオンプレミスとのハイブリッドなど、ユーザの要望に応じ、クラウドを柔軟に利用できるのがメリット。	・当初はコストメリットだったが、震災以降はコストだけではなく、災害対策としてメリットがでてきた。 ・あとは、アジリティやスモールスタート可能な面、システム全体で考えたときにオンプレミスとのハイブリッド運用などの柔軟性がメリットとしてあると思われる。	・コスト面がメリット。ユーザSIでシステム構築するよりもNTTコムのクラウドサービスを利用したほうがTCO3割以上は削減可能と考える。 ・また、グローバル展開の柔軟性というメリットもある。	・新規システム構築に対して当社がPaaSの標準PFを提供し、アジリティ、全体のコスト最適化（従来の基盤コストの3～4割削減）が図れる部分が利用者にとってメリット。
		クラウドサービス事業でメリットを生んだ実際の事例	・大手食品メーカーの基幹システム移行（保守サポート切れによる）：カットオーバーまで3か月間しかない中、一部試行から始め、逐次全面移行し、かつ TCO36％削減した。その間、目立ったトラブルはない。	-	・機械メーカーの事例：クラウドにフルアウトソースすることで、運用管理とコスト負担の抑制が実現（紹介資料あり）	・プラントメーカーの事例：新たなビジネスモデル立ち上げにクラウドが寄与。稟議通さずにクラウド利用でき、事業拡大に応じたシステム課金体系で、スモールスタートができたことがメリットであった。	・印刷業界のお客様事例：アジリティの部分でメリットがあり、競合他社よりも先に新サービスを展開できた。	・大手小売業の基幹システム：高信頼、かつグローバル対応できる点が大きく評価された。	-

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
		クラウドサービス事業にあたって考えられる経営的なメリット	–	・事業ポートフォリオという観点でメリットあり。 ・当社はずっと NW 事業をやってきたが、クラウド時代になり事業者側である程度汎用的に設計したものをユーザが利用するような環境になり、業務内容を拡大しやすくなっている。	・新規領域拡大と同時に本業へプラス(クラウド契約期間は長く、回線解約抑止にもつながる)	・ユーザへの新たな付加価値提供 ・クラウドを起点に派生ビジネス(コンサルティング等)が生まれている。	・クラウドサービスは、グローバルストラテジーの1つにも挙げられているほど重要な事業だと考えており、経営的なメリットは顧客満足度向上と新規顧客開拓(LOB)の2つと考えている。クラウドによりそれまでリーチしづらい顧客ともコンタクト取れるようになった。	・通信キャリアとして、もともとお客様の通信設備のアウトソーシングを請け負っており、クラウドサービスもその一環として展開できるので、全社シナジーが生かせる。	・当社のクラウドサービスは、他社 IaaS との価格競争と一線を画し、SI・アウトソーシング案件のシステム基盤部分に標準化されたクラウドサービスを組み込む方針で進めている。 ・これにより、これまでのスクラッチ型 SI から標準化クラウドへ変換することができ、低コストで高信頼性・高付加価値のシステム提供ができる。 ・また、顧客開拓、サービスを利用することによって自前主義からの体質改善ができる。これにより高付加価値分野に資源注力できる。
	リスク	クラウドサービス事業にあたって考えられる経営的なリスク	・大規模障害時の利用ユーザへの対応。数百社利用しており、各社担当者への連絡、対応のため、工数が膨大になる。	・クラウドは端的に言うと投資事業なので、投資リスクがある。今回の震災で DC は安全という認識がユーザには広がっているが、震災の影響でユーザが本社を国外に移転する動きがあり、国内だけでやっていくにはリスクがある。当社はそれに追従して海外にクラウド拠点を構築する計画でいる。	・投資リスクがある。ただ、アマゾン・ウェブ・サービス(AWS)のようにコンシューマー向けクラウドサービスとハードを共有することで、リソースの最適化が図れないか検討している。	・投資リスクあるのと、既存 SI 事業のシュリンクもリスクとしてある。既存事業のシュリンクについては、クラウドの派生ビジネス で補うことを考えている。	・現状の技術動向を考えると取り組まない方がリスク。当社は 2009 年にクラウド推進チームを立上げ、入念に準備をしてきた。SIとのカニバリする部分もあるが、バランスとってやっている。 ・財務的リスクよりも、顧客満足度低下のリスクが高いと考えている。	・クラウド事業は通信事業の延長上と考えており、投資リスクやシステムの大規模障害対応リスクはこれまでの経験上、ノウハウを持っている。	・当社クラウドは適正規模なので投資的なリスクや、SI とのシュリンクも少ないと考える。
		クラウドサービス事業にあたって考えられる災害やアクシデント等のリスク	・リソースの準備について、常に余裕を持って準備すべきだが、時として顧客の需要予測を超えた利用が発生することが	・大規模障害時の対応工数の増加、損害賠償リスクあり。クラウド事業規模はまだそれほど大きくないが、IT保険に入るなど	・データ消失リスクがあると考えており、現在3重でバックアップを実施。	・パブリッククラウドなので、大規模障害時に影響範囲が大きいのと、セキュリティアタックの影響も複数ユーザへ	–	・ただ、免責事項などは契約書で制限はしているが、ユーザのデータ管理について、クラウドになると管理レイヤーが上がる	・クラウドよりもどちらかというとデータセンターの方が、アクシデント等のリスクが大きいと考えており、震災時の対応を経験したことにより、さら

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
			あり、リソースの枯渇の恐れがある。	の対応は必要だと考えている。		波及するリスクがあると考えている。		ため、リスクがあると個人的に感じている。保険会社とリスクシェアしていくなど対策を検討していかなければいけないと感じている。	により良い災害対策を検討している。
		その他、リスクだと考えている事項	・クラウドの価格について誤解が生じやすい。自前構築と当社のクラウドサービスを比較する際に、忘れやすい電力代、スペース代等が自前構築に含まれておらず、クラウドサービスが高いという印象を持たれることが多い。	-	-	-	・クラウドサービスはITサービス調達の新しい手段であり、利用技術は発展段階のため。ベストプラクティスが業界で確立していない。	-	-
クラウドサービス事例	顧客の重要システム事例		・大手銀行のセキュリティ・キー・サービス、大手金融業の 401k の Web システム、大手食品メーカーの物流系基幹システム、県庁が中核の病院と連携して構築した救急医療情報システム等、公表できないのも含めると重要システムの事例は多くある。 ※活用事例の資料を受領。	・EC サイト、ゲームなど直接コンシューマーにサービス提供するシステムも停止すると、規模によっては億単位の損害が出るため、これも重要システムに該当すると思っている。 ・そういう意味で事例としては、ゲーム会社の事例が該当する。 ・その他 SaaS 型で金融事業社向けのサービス基盤も提供しており、フロントサービスからバックオフィス含めた領域も範囲となっている。コア事業の直結はこれからも進むと見ている。	・現時点では情報系がメインで重要システム事例は少ない	・ユーザ名は公表できないが、会計、販売管理、ERP 等の重要システムを当社のクラウドで運用する事例は出てきている。	・コラボレーションクラウド、デスクトップクラウドは金融等で利用されている。	・製造・流通業のお客様で基幹システムのクラウド化事例は少しずつ出てきている。ファーストリテイリング様など。 ・グローバル規模でサーバ基盤として使いたいというニーズもある。製造・流通は自前で DC を持ってない企業も多いので、基幹システムにクラウドを利用したいユーザはでてくると考える。一方で、金融は顧客が自前で DC をもっている点と、そもそものセキュリティポリシーの関係で、システムをクラウドで運用という話は少ない。	・オンラインバンキングと損保 ASP の事例がある。

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
	クラウド提供事業者からみて、顧客が重要システムを外部のクラウド上で運用しない理由を		・グループ会社にシステム会社があるところは自前主義。あとは、食わず嫌い・様子見。 →技術開発に関わる部分が当社のクラウドサービスにのらないのは、理系の人間が多く、自前主義の傾向が強いため。	・端的に言うと、ユーザのIT カルチャにつきる。 ・他社クラウド事業者の担当者も話していたが、信頼されるには、時間がかかる。まずは重要でない情報系システムの運用からはじまり、信頼を得ながら徐々に重要システムの運用を任せてもらうものではないかと実感している。	・一つは当社のサービスとして、瞬断も許されないようなアプリ向けの設計をメインとしていない部分がある。 ・情報系やメール等、短時間（再起動程度）であれば通信断が出てもいいようなシステムに利用してもらうようにしている。 ・もう一つはクラウドにすると責任の所在の問題が出て来る。当社に全て任せられるのかユーザが決めきれない。	・データを外部に預けることへのユーザの心配が障壁となっているのでは。企業のセキュリティポリシー上、情報を外部へ預けてはいけないとなっているユーザに対し、安心感を与えられていない。	・金融も利用し始めている。あとは共用度をどうするか。ユーザのセキュリティレベルに応じたメニュー作りが鍵なのではないかと思う。	・お客様にとって専用機器でのクラウド利用はハードル低いが、共有型は心理的な面でまだハードルがあるように感じる。 ・共有型はコスト競争力を高めるために信頼性やカスタマイズ対応など専用型に比べてお客様のニーズに対応しきれない面はあると考える。共有型サービスでも稼働率99.99%と謳っているが、たとえば病院だとそのレベルでは駄目で、ほぼ100%に近いものをお客様に求められる。そうすると、現状は専用型のオンプレミスになる。ただし、バックアップとしてクラウドを利用するという可能性は現状でも十分あると思う。	・顧客が重要システムに求める価値によるが、超高信頼、超高性能を求められるシステムは、クラウドはFitしない（ビジネス上成り立たない）。また、金融庁のお墨付きがないと困るという業態はまだクラウド利用には至ってないと考える。
今後のクラウドサービスについて	クラウドサービス事業の提供拡大の可能性とその理由		・クラウドの特徴であるアジリティが認められ、また自然災害対策機運も高まり今後も提供拡大すると見込んでいる。	・クラウド利用は今までノンコアの情報系がメインであったが、我々のユーザの中ではSAP に代表されるような会計、会社管理系の基幹システムをクラウドに移行する話も出てきており、今後も拡大すると思っている。	・足もとでユーザ数が増加していることもあり、今後も拡大すると考えている。	・インフラ技術としてクラウドがグローバル標準となっており、クラウドであればグローバル展開しやすく、ユーザのビジネス展開に連携しやすく、拡大していくのではないかと考える。	・足下の商談状況からも今後拡大すると感じている。	・今後クラウドサービスがますます展開していくことを睨み、当社ではグローバルクラウドビジョンを打ち出している。通信キャリアの強み生かし、OpenFlow 等の新たなネットワーク仮想化技術を使ってグローバルセンター間で仮想 NW を導入。それにより、グローバルな DC 間でリソース連	・時代の流れとして、所有から利用へという流れがあり、既存SIと組み合わせたハイブリッド型クラウドという利用形態が今後進むと思われるため、当社のクラウド事業も拡大していくのではないかと考えている。

インタビュー項目			DC・クラウド事業者回答						
大項目	中項目	小項目	A	B	C	D	E	F	G
								携、運用連携を実施していく。	
		今後クラウドサービスがより深く社会インフラへ浸透する上での展望および懸念	・今後クラウドサービスがより深く社会インフラに浸透するには、電力・通信等の他の社会インフラの提供価格を意識する必要があると思っている。	・今後クラウドサービスがより深く社会インフラに浸透するには、クラウドサービスに国がもう少し注力する必要がある（補助金を設けるなど）と思っている。 ・IT グローバル化の流れで、製造業等、海外依存度が高い企業がどんどん AWS を利用するようになると、AWS 内の情報が米国に渡るリスクを懸念している。 ・国策としてフォローすべき。電気代にしても海外の方が安価で、クラウド事業者も海外に拠点を作らざるを得なくなり、国内空洞化が一層進むことを懸念している。	・クラウドを意識させないことが今後深く社会インフラに浸透する上で必要だと考える。 ※NW の先、スマホの先にクラウドがあるようなイメージを持っている。 ・その際の懸念は大規模トラブル時。大きい流れではクラウド利用になっていると思うが、クラウドのトラブルが多発すると自社構築に流れが戻ると思われるため。	・クラウドサービスがコンシューマーに直接サービス提供できるようになると、もっと浸透していくと思う。スマートシティなど ・懸念は、いま無数あるクラウド事業者が今後淘汰されていくこと。当社が淘汰されないように強みを発揮していかないといけない。	・当社では新しいエンタープライズ向けのインフラのコンセプトを打ち出している。今後日本企業は海外進出が促進され、その際に上手くクラウドを活用できれば、さらにクラウドサービスが浸透するのではないかと思っている。 ・近頃インターネットベースでの安心・安全のバランスが崩れており、それがクラウドに波及することを懸念している。同じリソース共用サービスであるし。利便性とルールのバランスが重要（IPS/IDS のトレードオフなど）。今後のクラウドサービスは、価格競争よりも総合力なのではないかと考えている。	・今後クラウドサービスが社会インフラとして浸透するには、利用実績が必要。 ・情報系を皮切りに、ここ１，２年で素地がでてきたが、まだ基幹業務において活用されるレベルではない。 ・ユーザ間で情報交換が進み、もっと利用されていけば、クラウドはますます浸透していくのではないか。基幹系はこれからだと感じている。	・今後クラウドサービスがより深く社会インフラへ浸透するかどうかについて、現状ではクラウドに対する安心・安全の部分が、利用者に浸透していない。 ・展望として、クラウドは社会インフラになっていくものと考えているので、利用者が早くクラウドのようなサービス利用に慣れていく必要がある。

4. クラウドの機能停止が社会に与える影響の定性的評価

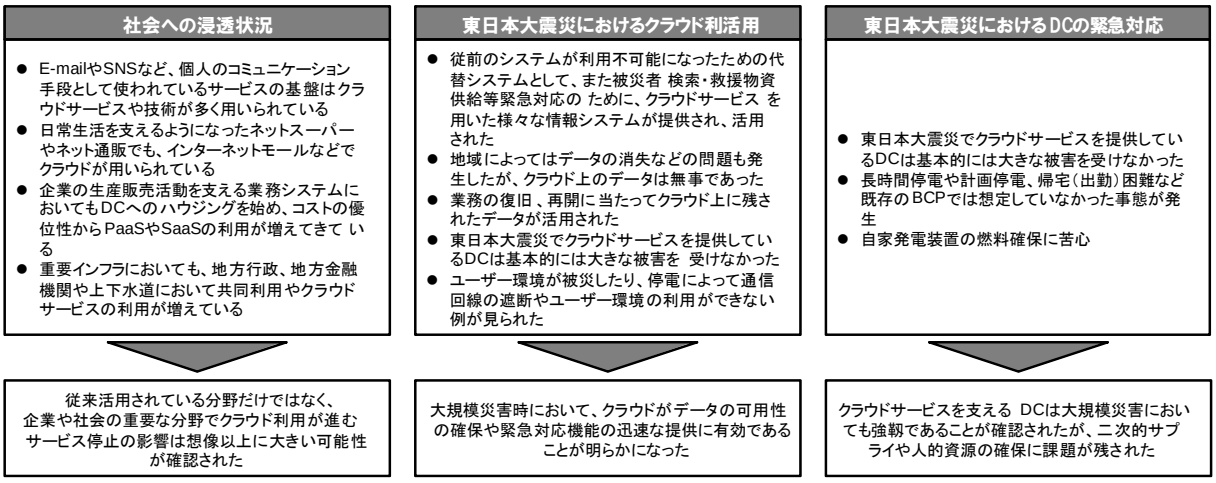
4.1. 実態調査のまとめ

本章の実態調査で明らかになったことを図表 92 に要約した。

まず、クラウドは個人・企業・社会のそれぞれにとって、重要なサービスの基盤を担いつつあるということである。そのことは裏返せばクラウドサービスが停止した場合の影響は、従来考えられていたよりも大きくなる可能性がある。

その一方で、東日本大震災の災害対応に際してのクラウド利活用の実態やデータセンターの緊急対応の状況から判断すると、大規模災害等における情報システムの可用性の確保や代替システム・機能の提供、復旧・復興に向けたシステム再構築に対して、クラウドが持つ特性が十分に役立つことが明らかとなった。情報セキュリティやデータ保存などの点からもクラウドが有利であったことも確認されている。

図表 93 実態調査から明らかになったこと



（DC：データセンター）

以下では、クラウドの社会への浸透、東日本大震災におけるクラウド利活用、東日本大震災におけるデータセンターの緊急対応の 3 つの視点から、実態調査で明らかになったことを述べる。

4.1.1. クラウドの社会への浸透

クラウドや ASP/SaaS、共同利用など、情報システムの構築・運用に当たって外部リソース提供サービスを利用することは、データセンターのスペースを借用して機器類をハウジングすることを除くとあまり進んではいない。アンケート調査の結果によれば、消費者向け EC では Web サイトにおける商品陳列などでも 25～30%であり、CRM 等の重要業務では 10～20%にとどまっている。また企業間取引においては、いずれの業務でもデータセンター

利用は 40%あるが、ハードウェアから上位の OS、プラットフォーム、アプリケーションのレイヤーになると 10～20%程度にとどまっているのが現状である。

ただし、重要インフラに関する事例調査で見たように、業界や業務によっては、外部リソース提供サービスの利用が大きなシェアを占めるものがある。具体的には以下のようなものである。

- 信用金庫の勘定系システムの共同化（90%）
- 地方銀行の勘定系システムの共同化（30%）
- 航空会社の業務システムのクラウドサービス利用（約 85 社）
- 上下水道遠隔監視クラウドサービス（293 自治体、6,000 施設に導入）

4.1.2. 東日本大震災におけるクラウド利活用

被災地を中心に、被災で利用が不可能になった既存の業務システムの代替や被災者支援・救援などを目的として、クラウドを用いた情報システムのサービスが発災直後から様々な主体によって提供された。このことにより、緊急時における迅速なシステムの立ち上げにはクラウドの活用が有効であることが改めて明らかとなった。

また、地域によっては既存システムに格納されていたデータが消失した例も報告されているが、一部のデータはクラウド上に保管されており、データの復旧に役立ったとされている。

一方、震災による主要なデータセンターへの被害はほとんど報告されておらず、機能を全うしたとされている。このことから、クラウドがサービスの可用性の確保に役立つことが確認された。ただし、停電による通信回線の遮断やユーザ環境の被災によって、サービスが利用できないケースが存在し、サービスの供給から消費までの全体としての継続性の確保が課題と言える。

4.1.3. 東日本大震災におけるデータセンターの緊急対応

前述したように、今回の震災においてはデータセンターに大きな被害はなかったとされる。ただし、被災による長時間の停電や関東における計画停電などの影響で、自家発電装置およびその燃料に対する課題がクローズアップされた。具体的には、自家発電装置の運転耐用時間の問題や緊急時における燃料の確保の困難さが指摘されている。

また、広範囲に及ぶ交通混乱によって保守運用要員の確保が困難になった事例もあり、今後の課題として認識されるようになった。

4.2. クラウド停止の影響

アンケート調査によれば、クラウドを利用している企業の企業間取引において、クラウドが停止した場合の影響は、調達の 40～45%、販売の 30～40%の取引（件数、金額、取引先数）に及ぶと回答されており、非常に大きいと考えられる。

このように、前述したクラウド利用のシェアが非常に大きい業務や業界では深刻な影響を受ける恐れがある。特に、金融機関、消費者向けEC等ではクラウドに依存するサービスが停止することによって、決済、現金の引き出し、日常必需品の買い物ができなくなる恐れがあり、国民の日常生活に非常に大きな影響を及ぼすことが想定される。

また、企業間の取引システムや情報共有システムなどにおいては、1 社の生産管理システムが停止して生産が止まるだけではなく、当該企業の下流のサプライチェーン全体に影響が及ぶ可能性も否定できない。東日本大震災では、システムが原因ではないものの、被災地の部品工場の生産が停止したことで、世界中の自動車生産に影響を与えた例が報告されており、情報システムの停止によっても同様のことが発生する恐れがある。

4.3. 最近発生したクラウドの大規模障害とそこから抽出されるセキュリティ課題

本調査の期間中に、災害以外の原因でクラウドサービスが停止する事例が複数発生している。ここではそれらの事例から社会システムとしてのクラウドに求められる課題を抽出する。

まず、構築したクラウドサービスのシステムが期待した性能を発揮できなかった結果、サービス直後から障害が多発した事例を取り上げる。この事例では、ストレージおよびストレージネットワークが原因でユーザデータの読み書きに障害が断続的に発生したうえ、復帰手順に人為的ミスが生じるなどが重なったため、ユーザデータを消去してしまい、復旧が不可能になるなどの問題が発生した。このストレージが正常に動作しない障害は発生以来半年以上にわたって断続的に発生し、根本的な解決までに非常に長い時間を要している。

第 2 の事例は、プログラム更新時のバグによってサーバ内の全データを消去してしまい、6,000 近くのユーザが保有する Web サイト、電子メール、グループウェア等のデータが復旧不可能になった事象である。また、バックアップを同一サーバ内の別ディスクに取っていたため、プログラムのバグによるデータ消去を防げず、バックアップの意味をなさなかった。このサービスは低価格で高いサービスレベルを売り物にしていたため、中小企業等の利用が多かった。これらの中小企業はITリテラシーも相対的に低く、ユーザ側でのバックアップがない場合も多かったという。そのためクラウドの障害によってデータがすべて失われてしまい、業務に大きな支障が出ているとの報告がある。これら 2 つの事例は、技術的に未熟な事業者のサービスによって、ユーザが期待する性能が提供できないばかりか、障害を引き起こし、ユーザの業務を停止もしくは大きく阻害する可能性があることを示している。

事例から抽出される課題は、「そのクラウドサービスの品質が優良なものであるかどうかをユーザが判断できる材料をどのように提供するのか」あるいは「サービスの品質を社会としてどのように確保していくのか」ということである。すなわち、最初の事例では、サービスを支えるインフラの質が不十分でサービスが断続的に停止してしており、これを外部から判

断することは難しく、また 2 番目の例では SLA では「100%稼働、外部バックアップ」を謳っていたものの、実態としてはそうではなく、障害時に対応が不可能になってしまっているため、SLA での判断は難しい。このような事例が引き続き起こるような状況が続けば、品質基準の策定と外部監査等の品質担保と表示のための仕組み作りが必要になってくる可能性がある。

第 3 の事例は、データセンターで電源トラブルによる障害が発生したため、ホスティングサービスが停止し、その上で提供されていた金融機関やクラウドサービス等のサービスが停止したものである。サービス停止の際、データセンター事業者はユーザ企業との責任分界点を考慮して、ユーザに対して停止を通知したものの、一般に向けてのアナウンスは行われなかった。ユーザであるサービス事業者ごとに、障害に関する説明内容やサービスの再開時期が異なるという問題があった模様である。しかし、今後緊急事態に近いレベルの障害が発生した場合の情報開示がそれだけでよいのかについては、検討の余地がありそうである。この事例から抽出される課題は、今後クラウド利用が拡大する中で影響範囲の広い大規模障害が発生した際の、時宜を得た情報開示の在り方とその方法の確立と考えられる。

以上のように、最近発生した障害事象から新たな課題が提起された。その課題とは、今後クラウドサービスは電力、水道、電話等と同等の社会基盤サービス（ユーティリティ）となっていくにあたって、「品質の保証はどのように行うべきか」「それはどのように担保されるべきか」「異常時におけるクラウド事業者の情報開示、すなわちリスクコミュニケーションはどのようにあるべきか」というものである。すなわちクラウドが社会に浸透して行くにつれて、クラウド事業者の供給者責任および、社会システムとしての担保の在り方はどのようにあるべきかを考えていく必要がある。

他の社会基盤サービス、たとえば電力事業などではある程度の独占性を事業者に認めた上で、品質管理責任を事業者に負わせている。また、運送事業では事業者の適格性を審査した上で免許を与え、必要に応じて監査を行う制度をとることによって品質の保証を行っている。さらに水道事業では国民の生命に直接関わることから、原則として市町村が経営すること[75]とされている。

同時に、各々の事業におけるサービス等の提供については、標準的な約款が用意され、供給側の供給責任の範囲、賠償等の限度や免責事項も規定されている。このことにより、生活必需サービスが異常な高コストとならないような安全弁も設けられている。クラウドサービス自体が生活必需の要素を持つケースはそれほど多くないとも考えられるが、それを利用する生活必需サービスは今後増加すると考えられ、そのコストとの兼ね合いで、この点も検討課題となろう。

このような事例も参考にしながら、クラウド事業の成長と両立する品質管理や供給者責任の在り方を検討することが求められる。

---

[75] 水道法第六条 2

II. クラウドが備えるべきレジリエンシ及びディペンダビリティを実現するためにクラウド事業者ならびに社会システムが満たすべき要件の調査

1. 問題認識

これまで述べてきたように、クラウドが社会に相当程度浸透していること、また東日本大震災においてもクラウドが果たした役割・機能が大きかったことが明らかになった。本章では、社会において少なからず重要な位置を占め、大規模災害時にも役立つクラウドの、大規模災害やセキュリティ障害に際してのサービス継続性を、どのように担保するかについて検討する。このために必要な要件や行うべき対策・取り組みは、一義的にサービスを提供しているクラウド事業者と利用者であるユーザ、さらには両者をつなぐ通信環境を提供している通信事業者が、その各々の責任において果たすことが求められるものと考えられるが、クラウドに電力等を供給しているライフライン事業者等に求められるものも考えられる。さらに、個々の事業者では取り組みが困難なものについては、行政の施策や社会全体の仕組みや制度として整備すべきものもあると考えられる。

調査の中では、東日本大震災級の災害状況を想定し、以下の要素について必要と考えられる対策ならびに要件を検討した。

- 平常時におけるライフラインの冗長性確保
- 緊急・災害時における代替ライフラインの確保
- 緊急・災害時における代替ライフライン確保のための二次的サプライの要件
- 通信回線に関する平常時ならびに緊急時の要件
- データセンターの運転ならびに保安のための要員に関する要件
- 意図を持って行われるサイバー攻撃に対する防衛または回避

2. 現状の取り組みと課題

1.で述べた問題意識をもとにクラウドの事業継続の観点から、現状の取り組みの状況と課題について整理する。

2.1. 対応の前提となる想定リスクの考え方を見直す必要性

東日本大震災では、従来は十分に想定していなかったリスクが数多く顕在化した。地震動や津波の直接の影響による施設の破壊・流失だけではなく、地盤液状化による施設の被害や長時間にわたる停電による影響も大きかった。その結果、通信回線が長時間にわたって遮断されたり、長時間にわたる停電に対応するための非常用電源用燃料の供給が十分に行き届かなかったりといった事態が生起した。また、南海トラフ巨大地震と首都直下地震の同時発生の可能性が排除できない[76]など、従来の想定を大きく越えたリスクの存在も具体的なものとなってきている。この教訓を踏まえて、従前の前提を疑い、リスクの洗い出しを再検討し、準備を充実させることは当然重要である。

しかしながら、そのようなアプローチのみでは、リスクや対策は言わば無限に広がり、大変複雑なものとなる。準備や対策に要するコストや手間も大きなものとなる。クラウド利用はIT の開発・運営のコストを縮減することが大きな目的となっていることを踏まえると、現実的には、準備・対応できることには限りがあることも確かである。

このような一定の制約条件がある中では、リスクの洗い出しと対策の立案においても、対応の考え方を変革していくことが重要ではないかとの有識者の指摘があった。

クラウドの利用目的や利用対象者は多様であり、それらに応じて平時におけるセキュリティ対策や災害時等の対策は異なる点に留意することや、リスク要因を網羅的に洗い出すのではなく様々な要因により共通して生じうる事象（たとえば、電源喪失）を想定した上で、そうした中間的な事象からBCP を検討すべきとの指摘がある。これらの指摘からの示唆は、想定外の状況があり得ることを想定して事業継続性を議論すべきであるということである。

また、実際に災害が起こった際には、被災状況や活用可能なリソースが刻々と変化するため、対応すべきリスクが絶えず変化する。このような状況においては、前もって定められた手順での対応だけでは限界があり、動的なリスクへの対応を図ることが重要になる。

---

[76] 2012 年 6 月現在、内閣府では、東海、東南海、南海等の連動型巨大地震災害に対する地震被害想定の見直し等を行っている。

2.2. データ・システムのバックアップの確保に関する現状

実態調査その 3 の調査対象の大手クラウド事業者については、図表 90 に示すように、デフォルト、オプションを合わせるとデータのバックアップ範囲は広く、別筐体のストレージや外部媒体、遠隔地バックアップも実施することが可能となっている。

図表 94 大手クラウド事業者のバックアップ対応（再掲）

事業者	A	B	C	D	E	F	G
データ保管対象（事業者範囲） ※デフォルト	ホスト OS レイヤーのシステムバックアップ、各種運用ログが対象	ホスト OS レイヤーのシステムバックアップ、各種運用ログが対象	・データの保管対象は、ファイルサーバの DR オプション契約分 各種運用に必要なログ（監視ログ、アクセスログ） 仮想サーバのスナップショット（IaaS,PaaS 系以外）。	ホスト OS レイヤーのシステムバックアップ、各種運用ログ、課金データが対象 ゲスト OS 以上のレイヤーが対象でユーザにてバックアップ	当社管理部分並びにユーザ作成分も含めた VM のイメージをバックアップしている。	-	ホスト OS レイヤーの各種運用ログが対象
データ保管対象（ユーザ管理範囲の代行保管） ※オプション	ゲスト OS 以上のレイヤーの各データ	ゲスト OS 以上のレイヤーの各データ	代行取得しない	代行取得しない	ユーザ管理の DB	ゲスト OS 以上のレイヤーの各データ	ゲスト OS 以上のレイヤーの各データ
保管データバックアップの有無	北海道データセンターに遠隔地バックアップ	遠隔地バックアップ	ファイルサーバの DR オプション契約分については DR サイトへバックアップ（遠隔地バックアップ）。 その他データについては、同一センター内の裏サーバへ Disk to Disk でバックアップ。	別筐体への DisktoDisk によるバックアップ。	ユーザバックアップ分については、別筐体に Disk to Disk でバックアップ 自社管理分については、外部媒体へバックアップしている。	ユーザ指定で Disk2Disk、テープ、遠隔地バックアップが可能。	データバックアップについて、同サイト内に保管。 今後遠隔地バックアップ予定
保管データ量及び増加スピードについて	回答差し控え	保管データは数ペタバイトのレベル。スピード感としては年ごとに倍増。	保管データ量については開示できないが、増加スピードは、昨年から1年間で 6 倍増えている。	ビッグデータソリューションの引き合いもあり、データ量はかなりある。テラバイトクラス。	保管しているデータ量および増加スピードについては、クラウドサービス全体では数ペタバイト、当該データセンターだけでも数百テラバイトが利用されている。	回答差し控え	回答差し控え
保管期間	回答差し控え	データ保管期間の制限は現状設けていない。	データ保管期間について、ファイルサーバの DR オプション契約分はユーザ契約期間	明確に決まってないが、大体 5 年間。	回答差し控え	オプションにて、ユーザ指定可能	ユーザデータ分は契約期間中ずっと保管。 事業者側の構成情報について、サービス提

事業者	A	B	C	D	E	F	G
			まで。運用ログの保管期間は定めていない。VM のスナップショットは1世代分。				供中は保管し、世代管理を実施。
復旧方法	NW 越しにバックアップデータ送信し、リストア	データ復旧はリストア	データ復旧はリストア	データ復旧はリストア	事業者管理データの復旧方法については、回答差し控え ユーザ管理範囲のゲストVMのデータのバックアップとリカバリーはユーザ責任で行う必要があり、そのための手段として専用ソフトを提供	データ復旧はリストア	データ復旧方法について、ユーザデータ分はユーザがリストアできるように API、画面を提供。事業者分はリストアにて復旧。

出所）実態調査（その 3）によるインタビュー結果から NRI 作成

しかしながら、中小、新規事業者の中には大規模障害事例で見られたように、十分なバックアップ体制を取っていない可能性は否定できず、適切な情報開示が求められる。情報開示に関しては、総務省と NPO 法人 ASP・SaaS・クラウドコンソーシアム（ASPIC）が 2011 年 12 月に「データセンターの安全・信頼性に係る情報開示指針（第 2 版）」および「IaaS・PaaS の安全・信頼性に係る情報開示指針」を策定している。

「データセンターの安全・信頼性にかかる情報開示指針（第 2 版）」の 118 項、「IaaS・PaaS の安全・信頼性に係る情報開示指針」の 41 項で「バックアップ・リストアサービス：バックアップ、障害時のリストアサービスの内容」を定義しており、今後バックアップに関する情報の開示が期待される。

また、一般財団法人マルチメディア振興センターが「ASP・SaaS 安全・信頼性に係る情報開示指針（第 1 版）」（2007 年 11 月総務省）に基づく認定制度を行っており、同センターのサイトで、認定を受けたサービスの情報開示を行っている。ASPIC へのインタビューでは、上記の「データセンターの安全・信頼性に係る情報開示指針（第2版）」および「IaaS・PaaS の安全・信頼性に係る情報開示指針」による情報開示適合認定も検討中とのことであり、外部認証による品質保証の強化も期待される。

2.3. BCP（事業継続計画）による準備の現状

前項と同様、インタビューを行ったデータセンター事業者については、各社とも緊急対応マニュアルを用意しており、一定程度の対応は行われていた。具体的には、災害対応フロー、緊急対応マニュアル、安否確認システム、初期の損害チェックリストなどが含まれている。

図表 95 大手データセンター事業者の BCP 対応状況（再掲）

A	B	C	D	E	F	G
震災前にマニュアル準備済み	震災前に以下準備済み ※災害対応フロー、緊急対応マニュアル、安否確認システムなど	震災前に以下準備済み ※全体フロー、安否確認システム、初期損害チェックリスト。	震災前にマニュアル準備済み。	震災前にマニュアル準備済み。	震災前にマニュアル準備済み。 ※大規模障害時のノウハウは溜まっており、それを元にしたマニュアルがある。	震災前に以下準備済み。 ※安否確認システム、地震発生時の確認リスト。

出所）実態調査（その 3）によるインタビュー結果から NRI 作成

また、前項と同様に総務省およびASPICが策定した2種類の情報開示指針において、「事業継続に関する規程等の整備」として「事業継続に関する基本方針、計画、マニュアル等の文書類の有無と、有りの場合は文書類の名称」（28 項）および「上記の文書類の経営陣による承認の有無」（29 項）が定義されており、これに沿った情報開示が期待される。

2.4. 平常時からのファシリティ面の対策

日本データセンター協会（JDCC）では、図表 95 に示すように「JDCC データセンターファシリティスタンダード」を制定し、データセンターの重要度（ティア）別に、建物、セキュリティ、電気設備、空調設備、通信設備ならびに設備運用について満たすべき基準を定めている。 法令で定められた建築基準においては、データセンターに特別の厳格な基準や規制が加えられているわけではないものの、各事業者において、上記のファシリティスタンダードに基づいて、堅牢性を確保している。前述したように、東日本大震災ではデータセンターは、ほとんど無傷で、事業継続できたことが確認されており、ファシリティスタンダードが有効であったことが改めて確認された。

しかしながら、いくつかの課題が認識されている。まず、件数は少ないものの、サーバ室の天井が剥がれ落ちたケースと免震構造のサーバーキャビネットが倒れたケースが見られた。また、データセンターには被害が及ばなかったものの、津波による浸水・流失や埋め立て地等における地盤液状化によって建築に大きな被害がもたらされた。従来のデーターセンターファシリティスタンダードではこれらの点については十分考慮しておらず、今後対策を強化すべき課題として認識された。

図表 96　JDCC ファシリティスタンダード（基準項目一覧）

分類	No.	評価項目	ティア 1	ティア 2	ティア 3	ティア 4	備考
建物（B）	1	建物用途 （建物としてDC専用であるか否か）	複数用途 複数テナント可	複数用途 複数テナント可	複数用途 単一テナント	DC専用 DC関連複数テナント	
	2	地震リスクに対する安全性 1）PMLによる評価の場合	PML 25～30%未満	PML 20～25%未満	PML 10～20%未満	PML 10%未満	
		2）建築基準法による評価の場合 ※1：官庁施設の総合耐震計画基準及び同解説（建設大臣官房官庁営繕部監修、平成8年版）高さ60mを超える高層建築物、免震建物はⅠ類 ※2：今後50年間に10%の確率で発生する可能性のある予測震度（文部科学省 全国地震動予測地図）	1981年以前の建築基準法に準拠 耐震診断の結果、耐震補強不要と判断された場合 耐震補強が必要と判断され耐震補強を実施済みの場合		1981年6月改正の建築基準法に準拠	1981年6月改正の建築基準法に準拠、かつ耐震性能はⅡ類相当※1	震度※2 6弱以下
			1981年以前の建築基準法に準拠 耐震診断の結果、耐震補強不要と判断された場合 耐震補強が必要と判断され耐震補強を実施済みの場合	1981年6月改正の建築基準法に準拠	1981年6月改正の建築基準法に準拠、かつ耐震性能はⅡ類相当※1	1981年6月改正の建築基準法に準拠、かつ耐震性能はⅠ類相当※1	震度※2 6強以上
セキュリティ（S）	1	セキュリティ管理レベル	サーバ室	サーバ室	建物、サーバ室	敷地、建物 サーバ室、ラック	
電気設備（E）	1	受電回線の冗長性	単一回線		複数回線（SNW、本線予備線、ループ）		
	2	電源経路の冗長性 （受電設備～UPS入力）	単一経路	単一経路	複数経路	複数経路	
	3	電源経路の冗長性 （UPS～サーバ室PDU）	単一経路	単一経路	複数経路	複数経路	
	4	自家発電設備の冗長性	規定無し	N	N	N+1	
	5	UPS設備の冗長性	N	N	N+1	N+2	
空調設備（H）	1	熱源機器・空調機器の冗長性	N	N	N+1	N+2	
	2	熱源機器・空調機用 電源経路の冗長性	単一経路	単一経路	複数経路	複数経路	
通信設備（T）	1	引き込み経路 キャリアの冗長性	単一経路 単一キャリア	複数経路 単一キャリア	複数経路 複数キャリア	複数経路 複数キャリア	
	2	建物内ネットワーク経路 の冗長性	単一経路	複数経路	複数経路	複数経路	
設備運用（M）	1	常駐管理体制	規定無し	規定無し	8時間/日以上の常駐管理	24時間×365日の常駐管理	
	2	運用マネジメントの仕組みと運用 （運用要員の育成プログラムなど含む）	運用体制有り	運用要員育成プログラムを含む規定された運用体制有り	ISO27001又はFISC運用基準において、設備運用に関する項目に準拠	ISO27001の認証又はFISC運用基準に準拠	

出所）JDCC　データセンターファシリティスタンダード（概要）

2.5.　平常時におけるライフラインの冗長性確保

東日本大震災では仙台の変電所が水没、停止したため、電力の復旧に時間を要した。データセンターのファシリティ面よりは、ライフラインに対する準備がボトルネックとなる可能性が改めて認識されている。

慶応義塾大学の大林厚臣教授によると、情報システムはBCPによる平常時の準備の効果が現れやすい領域である。BCP では代替性がポイントとなるが、代替機やデータバックアップなど、情報システムは代替性を前もって確保しやすい領域であるためである。

ただし、現状ではクラウドサービスすべてにわたって代替性や冗長性が確保されているとは限らない。たとえば今回の震災においてもクラウドを運用するデータセンターとユーザ間の通信回線に冗長性がなく、サービスは提供されていたがユーザが利用できない例が見られた。しかし、冗長性の確保にはコストがかかるため、東京電機大学の佐々木良一教授へのインタビューで指摘されたように、ユーザのクラウド利用の動機で最も強いものは情

報システムのコスト抑制であり、コストと冗長性の確保をいかに両立させるかが課題である。

2.6. 緊急・災害時における代替ライフラインの確保

非常用の自家発電機は累積運転時間が一定の時間に達すると耐用時間を越えるため、オーバーホールを行う必要がある。JDCC によると、長時間に及ぶ電力供給の停止は、以前はデータセンターの多くは全く想定していなかったが、今後は想定すべきではないか、とのことである。

また、緊急・災害時には通信回線の確保に加えて、その容量も問題となる可能性がある。陸前高田市では Web サーバを市外のデータセンターで運用していたため、Web ページ自体は稼働を続けていたものの、サーバまでの通信回線が断絶し、衛星電話を用いたダイヤルアップで情報更新を行った。このため、大容量のコンテンツを更新することはできなかったという。

通信回線の多重化と容量の確保や非常用電源の強化など、緊急・災害時における代替ライフラインの確保に向けた対策については、クラウド事業者、通信事業者等が一義的に行うべきことである。また、これらの対策を取っていることをユーザに適切に開示することが求められる。

2.7. 緊急・災害時における代替ライフライン確保のための二次的サプライの要件

東日本大震災の教訓のひとつは、データセンターのファシリティとしての堅牢さだけでは対策は十分ではなく、非常用電源を動かすための燃料が重要であるという点である。JDCC によると、被災地のデータセンターは燃料の備蓄が一定程度あり、補給でなんとか稼働し続けたが、一部銀行の電算センターでは3時間程度の燃料備蓄しかなく、停止した。これは、リスクの想定として、電力の供給が停止する可能性があることを見越して準備していたかどうかによる差であった可能性がある。

また、燃料の優先供給契約があまり機能しなかったことも判明した。石油連盟によると、タンクローリーの不足、交通遮断、被災地への優先的供給などが要因であった。また、燃料供給者の視点からは、各所から要望が殺到する中で優先順位を付けて供給することは民間では無理がある。先の震災では内閣府防災担当からの要請順位に基づいて供給を行ったという経緯であった。ただし、供給先の輸送条件(タンク容量・形式、道路条件等)がわからないまま行ったために空振りも多数発生したとのことであり、事前の情報共有・把握が重要であると考えられ、石油業界においても取り組み[77]が始められつつある。

2.8. データセンターの運転ならびに保安のための要員に関する要件

佐々木教授、大林教授、JDCC、各データセンター事業者へのヒアリングによると、データセンターの建物がいくら強固であっても、システムを動かす要員が緊急・災害時に集まる

[77] 石油連盟「災害時の重要施設に係る情報共有に関する覚書の締結について」(2012 年 3 月 29 日)
http://www.paj.gr.jp/paj_info/press/2012/03/29-000565.html(2012 年 6 月現在)

ことができるかという点は大きな課題である。今般の震災では金曜の昼間であったため深刻な問題とならなかったものの、夜間や休日であった場合の要員参集の困難が懸念される。また、交通寸断により要員確保が難しくなるケースも想定される。

3.11 のときは大きな問題とならなかったが、大規模な自然災害の後にインフルエンザなどの感染症が広がるリスクもある。大林教授によると、東日本大震災では医療や福祉関係者が相当感染症の予防に気を付けていたとのことである。仮に感染症が広がった場合、要員確保は一層困難となる。

このようなリスクを踏まえると、緊急・災害時においては平時よりも大幅に少ない要員でクラウドの継続、または早期復旧に向けた対策を講じなければならない事態が想定される。しかしながら、企業等のBCPでは要員参集に関する前提や想定に課題が残る事例も見られる [78]。少ない要員での事業継続、ないし要員参集を前提としない事業継続の方法等を準備することが課題である。

東日本大震災においても、あるクラウド事業者が東北地方のデータセンターにおいて、要員の住居の被災、家族の安否確認に加えて、交通機関の麻痺などが起こり、要員の確保が困難となったため、発災後数日以内に西日本のデータセンターの要員による遠隔運用に切り替えている。このように、遠隔運用を行えるような設備、要員の訓練等の備えが求められよう。

2.9. 緊急・災害時におけるセキュリティ対策、ならびに意図を持って行われるサイバー攻撃に対する防衛または回避

緊急・災害時には厳重なセキュリティチェックが難しくなるケースがある。たとえば、自家発電装置への燃料補給のためにデータセンターへの入館を比較的容易に認めるといったケースも想定される。この際に、緊急対応のためのデータセンターへのアクセシビリティの確保とセキュリティの確保を、どのように両立させるのかを、クラウド事業者は前もって考えておかねばならない。

一方、災害発生時には、平常時のセキュリティレベルを下げる必要のあるデータも存在する。たとえば、医療における患者データの共有がクラウドで円滑に進むと、人命救助等の点で効果的である。これについては、データを保有するユーザが決定してクラウド事業者に指示することで可能になると考えられるが、緊急時に個別判断を集めること、複数患者の合意形成を図ることは現実的でない。個人情報や機微な情報に関してセキュリティレベルを下げることについて、社会的なコンセンサスの形成が必要になることを想定しておく必要がある。また、緊急事態が収束して平常状態に復するときには、緊急対応で拡大した開示範囲に残存するデータの回収や抹消も行わなければならない。緊急対応で拡散したデータのトレーサビリティは低いことも想定され、一定条件下での一斉消去等、その方策や判断基準も予め整えられていることが必要になる。またそのような緊急対応とその収束に

[78] 浅野憲周「事業継続計画（BCP）再考－大震災から企業は何を学ぶべきか」知的資産創造 2012 年 2 月号

際しての、開示・回収・消去の手続きや判断結果に関する、セキュリティ監査や監視を誰がどのような手順で行うのかについてもユーザ、クラウド事業者および社会全体で合意を形成する必要がある。

クラウドにおいてもサイバー攻撃等に備えた対策としての基本的な事項は、アクセス制限やデータの暗号化など通常の情報システムの場合と同様であるとの有識者の指摘がある。システム運用の視点で見た場合、複数のシステムを集約的に運用するクラウドでは、個別分散的にシステムを運用する場合に比べて高度な情報セキュリティ対策を集約的に導入できるため、セキュリティレベルが高くなるとも考えられる。しかしながら、セキュリティが破られた場合の影響範囲が大きくなるため、クラウド事業者の情報セキュリティ確保への不断の努力が求められる。と同時に、ユーザの以下のような懸念への対応も必要となる。

第 1 に、データ/システムをクラウドに置いた場合、自社のシステム内で閉じている場合よりも攻撃の対象となりえる可能性が増えるということを意味する。

第 2 に、クラウド事業者にデータやシステムの運用を任せるため、ユーザの IT リテラシー、とりわけセキュリティに対するものが低下する可能性が高い。また、クラウド化されると、ユーザにとってはその先では何がどのように行われているか見えないため、セキュリティ管理の経験や学びの機会が減る。したがって、ユーザに対するセキュリティ教育は重要な課題のひとつである。

さらに、大規模災害時の混乱に乗じたサイバー攻撃等も視野に入れる必要がある。災害対応でシステムが脆弱になり、要員が手薄になったところで攻撃された場合の対応など、複合的なリスクへの対応を検討しておく必要があると考えられる。

2.10. 中小事業者、ベンチャー等の提供するクラウドサービスのリスクへの対応

最近のクラウドの大規模障害事例では、中堅企業が提供するサービスに重大なトラブルが起き、ユーザに甚大な影響を及ぼしたことが報告されている。今後もクラウドサービスに新規に参入してくる事業者が増えるものと思われ、その中には中小企業やベンチャーなど企業体力が必ずしも強くない事業者も増えてくると考えられる。新規参入は市場や経済の活性化のために歓迎すべき事象ではあるが、インフラ的性格を持つクラウドにおける品質の確保との両立が課題となる可能性も否定できない。今後は、これらの企業の技術面での未熟さなどのリスクばかりではなく、財務面でのリスクも考慮する必要が出てくる。

たとえば、このようなクラウド事業者が大規模な障害を起こして損害賠償に応じなければならないケースや、経営が行き詰まって倒産するケースを想定し、責任の所在を明確にしておく必要がある。大林教授、佐々木教授によると、契約（SLA 等）でどれだけリスクに備えた対策を盛り込めるかがポイントとなる。

これに備えた保険等の経済的セイフティネットの整備や、サービスの利用継続に向けてのユーザの救済方法の検討も求められよう。たとえば、旅行業においては、中小事業者の倒産リスクを業界全体で負担するため、旅行業法に基づく「弁済業務保証制度」や日本旅

行業協会の独自の制度である「ボンド保証制度」によって消費者の保護を図っている。このような取り組みを行うことによって、ユーザの信頼感を高めていくことが可能になるとも考えられる。

3. クラウド事業者ならびに社会システムが満たすべき要件

3.1. 想定外のリスクならびに動的なリスクへの対応

前節で抽出した課題では、個別の取り組みもさることながら、想定外のリスクや動的なリスクへの対応の考え方の整理が重要であることが明らかになった。この点につき、佐々木教授、大林教授らの指摘を踏まえて整理したものが図表 96 である。

以下、この流れの要点についての詳細を記述する。

3.1.1. 一定の条件設定に基づいたリスクの洗い出しと対策の立案

従来の BCP の枠組みでは、想定されるリスクを網羅的に洗い出し、対策を準備するというアプローチが多かった。しかしながら、そのようなアプローチのみでは、リスクや対策は言わば無限に広がり、大変複雑なものとなる。準備や対策に要するコストや手間も大きなものとなる。クラウド利用は IT の開発・運営のコストを縮減することが大きな目的となっていることを踏まえると、現実的には、準備・対応できることには限りがあることも確かである。

リスク要因を網羅的に洗い出そうとするよりは、様々な要因により共通して生じうる事象を起点に BCP を策定することも必要である。たとえば、電源供給遮断や運用要員が参集できないなどの中間的な状況から対応を検討する。もちろん、その電源供給遮断の原因が送電網の被災か、受電施設の浸水かなどによって対応は変わってくるが、検討するリスクを無限に広げないために、一定の枠を決めることは重要であると考えられる。

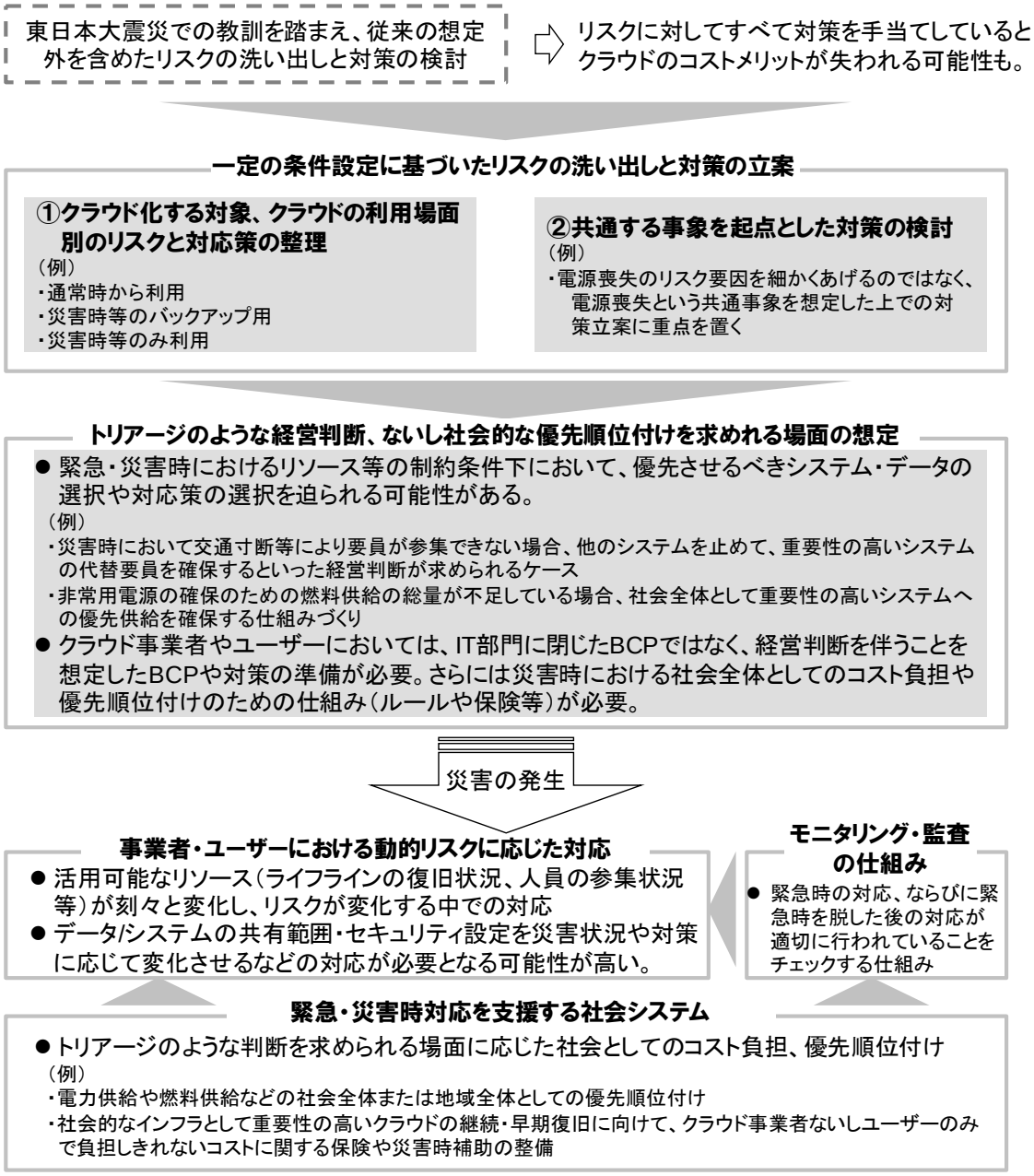
3.1.2. 優先的に稼働させるシステムの選定とステークホルダー間の合意形成

(1) 基本的な考え方

長期間にわたって電力が復旧しない、あるいは十分な要員が参集しないなど、クラウドの運用に必要なリソースが極端に制約された条件下において、大幅な縮退運用を余儀なくされるケースが想定される。その結果、クラウド事業者やユーザが運用継続を優先させるべきシステムの選択を迫られる可能性がある。

また、東日本大震災でクラウドサービスが数多く提供された例に見られるように、緊急時にはその対応のために、新たな情報システムのニーズが多数・多様に発生すると考えられ、その多くが平常時のシステムより高い緊急度・優先度をもつ可能性が高い。

図表 97 事業継続の観点からのクラウド事業者等が準備・対応すべき対策の流れ(例)



医療においては災害時等に治療の優先順位付けを行う「トリアージ [79]」という概念があるが、これと同様に前もって判断基準のみを策定しておき、事象が発生した際にはその判断基準によって優先順位付けを行うことが考えられる。それにより、たとえば重要インフラを支えるクラウドの復旧を優先させたり、緊急度の低いサービス(たとえば音楽配信など)向け

[79] triage:フランス語で「選別」「優先割当」の意。医療において、大規模災害が発生したときに、負傷の度合い等から治療の優先度の高い患者を判別すること。通常は、判別する医療従事者が結果をタグなどで表示し、救急隊や治療する医療従事者に容易に引き継げるようにする。

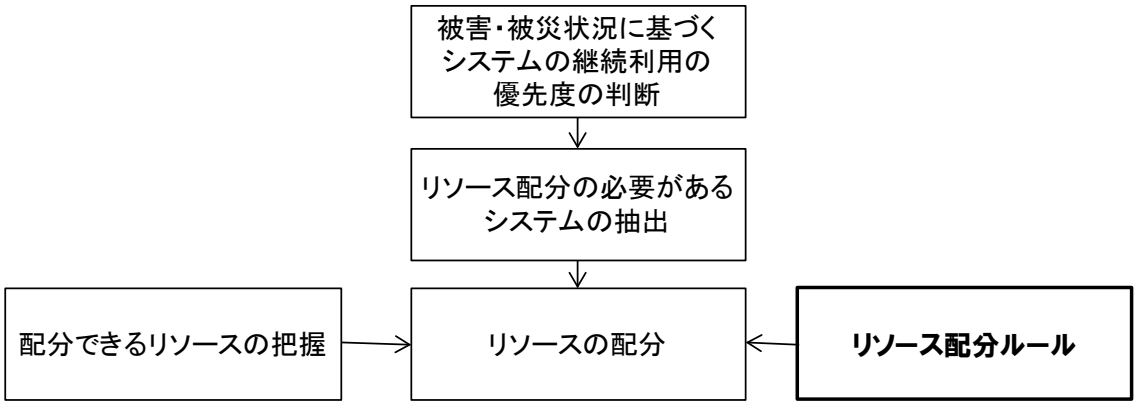
のリソースを絞って、被災者支援情報システムや救援物資物流管理システムを緊急に立ち上げたりするなどの対応が可能になる。このようなシステムの「トリアージ」においては、共用サービスであるクラウドならではの問題が発生する可能性がある。すなわち、オンプレミスのシステムであれば、当該ユーザのみの判断で「トリアージ」を行うことが可能であるが、一つのインフラを共用している複数のユーザのサービスにまたがる問題であるため、ユーザ間の調整が必要になると考えられる。

(2) 優先順位を判断する手順

具体的には図表 97 で示すような手順で、優先して稼働させるシステムを抽出し、リソースを配分する。前もって、リソース配分のルールを策定しておき、災害や障害が発生した際には、システムの被害・被災状況を勘案して、クラウド上のシステムの継続利用について優先度の判断を行う。

同時に、配分できるリソースの把握を行って、前もって策定したルールに従ってリソース配分を行うこととなる。

図表 98 リソース制約下におけるリソース配分の手順の例

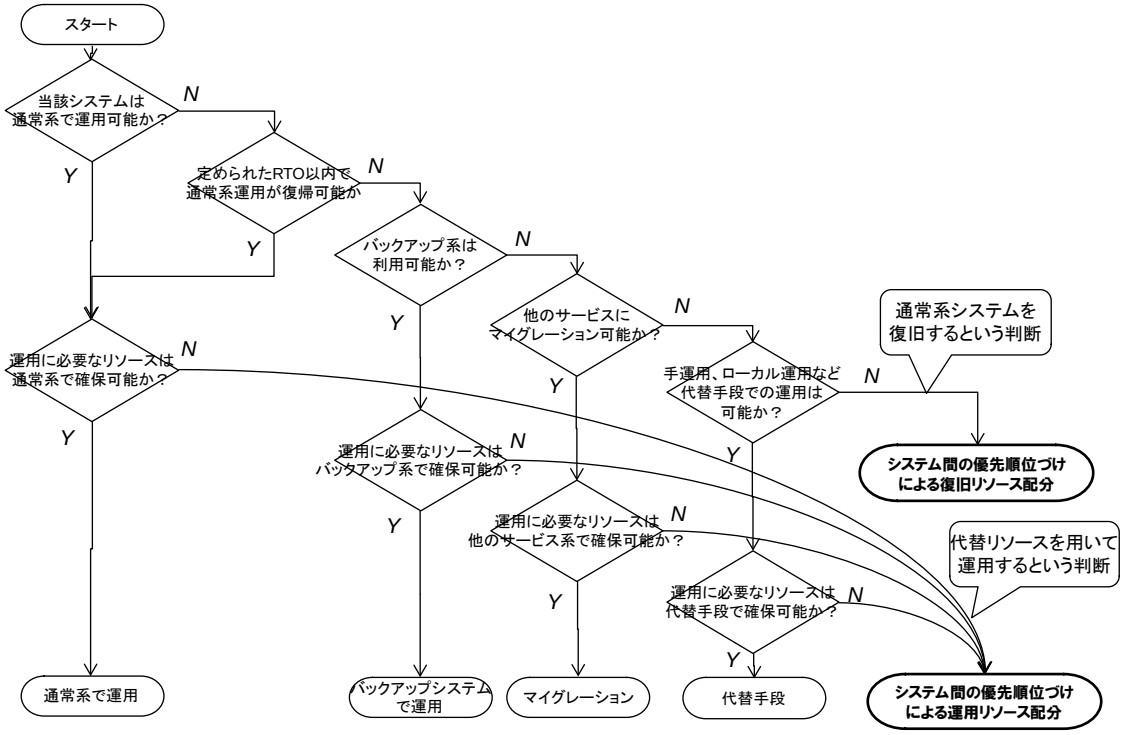


(3) 配分できるリソースの把握とリソース配分の必要があるシステムの抽出

このうち、配分できるリソースの把握については、図表 98 に示すようなステップで行うことができる。当該システムの通常系、バックアップ等の代替手段の利用可能性を順次検討して行き、次いでその手段を運用するのに必要なリソースが通常系で確保できるか否かを判断する。停電している、通常シフトの運転要員が出勤できないなど、リソースが通常系で確保できない場合に、代替リソースの配分対象の候補となる。

なお、リソースが通常系で確保できるか否かについて把握する方法は平常時から定めておく必要があり、クラウド事業者へのインタビューでも、非常用発電機の燃料や飲料・食料の備蓄量の確認はもちろん、事業者によっては運転要員の安否・出社可否等を把握するシステムを導入するなどの方策をとっている。

図表 99 システム利用継続性の判断フローの例



(4) リソース配分ルールの策定

一方、事前に定めておくリソース配分ルールの検討に当たっては、図表 99 に示す業務とシステム両面にわたる事項を考慮する必要があるものと考えられる。

業務面においては、当該システムが支援する業務の優先度を考慮する必要がある。。発生した事態への応急・緊急対応が必要である業務や、人命に関わる業務、法令等で定められている業務などが優先度の高い業務と考えられる。このような業務の優先度を把握する指標として、業務そのものの RTO（Recovery Time Objective）などを参照することが望まれる。

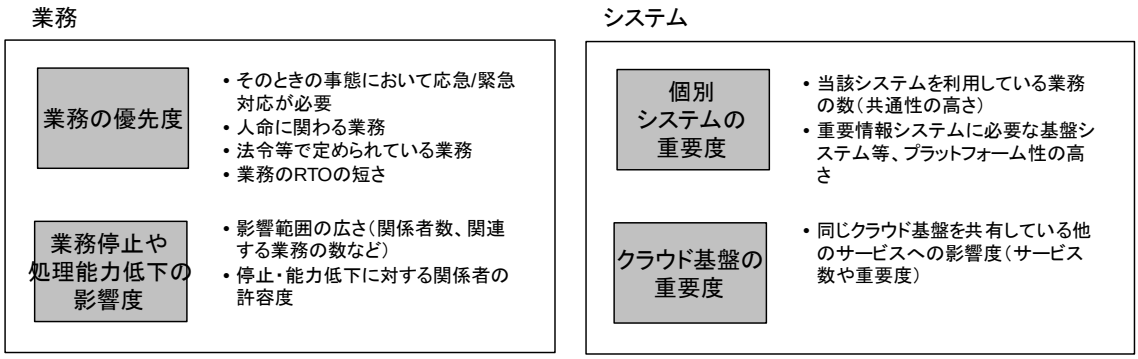
また、システムの不稼働による業務停止や処理能力低下の影響度を考慮に入れる必要がある。影響度の指標として関係者数や関連する業務数、あるいはその業務の内容などを参照する。たとえば生産管理システムであれば業務が停止してしまうことでサプライチェーンの下流に大きな影響を与える。同時に業務停止や能力低下に対して、関係者がどれだけ受容できるかも考慮に入れる必要がある。

システム面については、個別システムの重要度とそのシステムが存在するクラウド基盤の重要度を合わせて考慮する必要がある。個別システムの重要度では、当該システムを利用している業務数など、そのシステムの共通性の高さや、重要な情報システムが当該システムに強く連携しているなど、プラットフォームとしての重要性を合わせて検討すべきである。

クラウド基盤の優先度を考える上では、重要インフラや重要システムが稼動しているクラ

ウド基盤の回復と継続が優先される必要がある。同じクラウド基盤から提供されるサービスを絞る必要がある場合は、同一基盤を共有している他のサービスやシステムへの影響度を考慮に入れる必要がある。

図表 100 リソース配分ルールの策定に当たって考慮すべき事項



(5) 配分するリソースの把握

配分するリソースがどこにどれだけ存在するのかを的確に把握することが必要だが、非常時に初めて情報収集をするのでは混乱する可能性が高い。そのため、平常時から情報ルートを定めておくことが望ましい。

本章 2.7. において触れた非常用発電機の燃料確保について、石油連盟は東日本大震災の経験を踏まえ、石油元売り各社の備蓄量の把握だけではなく、地方自治体と協定を結び、供給の必要が想定される施設について、タンクの容量や供給口の形状など輸送要件についても事前に情報の集約を図ろうとしている。このように、リソースの所在・量だけではなく、OS やユーティリティの種類、API やデータフォーマットの互換性など、緊急利用や代替提供に必要な要件についても事前の情報収集を進めておくことが望ましい。

(6) ルールの策定やリソース配分の主体

以上述べてきたような優先順位の決定やリソース配分の調整は、クラウド事業者で完結できる場合もあれば、そうでない場合もある。

他のデータセンターからの要員や燃料の融通などクラウド事業者で完結できる場合は、クラウド事業者の判断でリソース配分できる。しかしながら、電力や非常用電源の燃料など、他の業界と共用しているリソースについてはクラウド事業者のみでは行いきれず、クラウド事業者およびリソースの供給事業者・業界団体、行政なども含めて検討していくことが有益であると考えられる。たとえば、非常用電源の確保のための燃料供給の総量が不足している場合、社会全体として重要性の高いシステムへの優先供給を確保しなければならない。東日本大震災の事例では、石油連盟および全国石油商業組合連合会が業界として供給責任を担ったが、優先順位の判断は民間では行いきれないため、政府の指示による優先順位従って供給を行っている。

このように、トリアージを行うに当たっては「誰が」「どのような条件で」「どんな情報に基づ

いて」「どんな権限によって」優先順位を判断し、「誰が」「どのように」実行を指示するのかがあらかじめ決められてあり、共通認識になっていることが重要である。そのための社会的な仕組みづくりや合意形成を平時から進めておくことが必要となる。判断、指示の体制は、混乱を拡大しないためできるだけシンプルにしておく必要があると考えられるが、判断・指示をする担当者に事故があった場合に備え、権限委譲の順位を定めるなどの対応も必要である。

（7） その他の要件

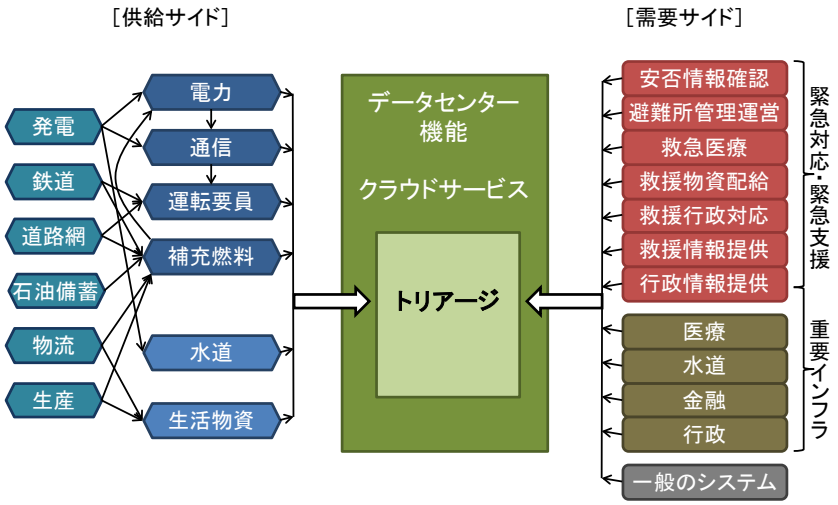
この判断基準について、柔軟性をもった判断やトリアージとも言える場面での経営判断が適切に行われているかどうかについては、モニタリングあるいは監査を受けることも必要ではないか、という点が佐々木教授からは指摘された。とりわけクラウドにおいては、ユーザにとってはシステムの状況やクラウド事業者の対応の状況は見えにくいため、クラウド事業者の対応をチェックする仕組みの構築は通常の情報システムと比べても大きな課題である。現行の情報開示制度をさらに充実させることも必要と考えられる。

また、必要なコストについてはユーザへの料金に転嫁されるものと考えられるが、ユーザニーズである低廉なシステム利用コストとのバランスを考慮する必要がある。保険のような仕組みを組み入れることが有効である可能性もある。今後の検討課題と言える。

3.2. トリアージの枠組みにおける考え方の例

ここでは、3.1 で考察した緊急時におけるデータセンター機能の維持・提供に関する「トリアージ」的アプローチの例示を試みる。医療における緊急時の救急治療の優先度を判断する仕組みの概念を援用して、ここでは「前もって判断基準のみを策定しておき、事象が発生した際にはその判断基準によって優先順位付けを行うこと」の意味を持つものとして使用する。その考え方の枠組みは、図表 97 のように表わされる。

図表 101 データセンター機能に関するトリアージ的判断枠組み

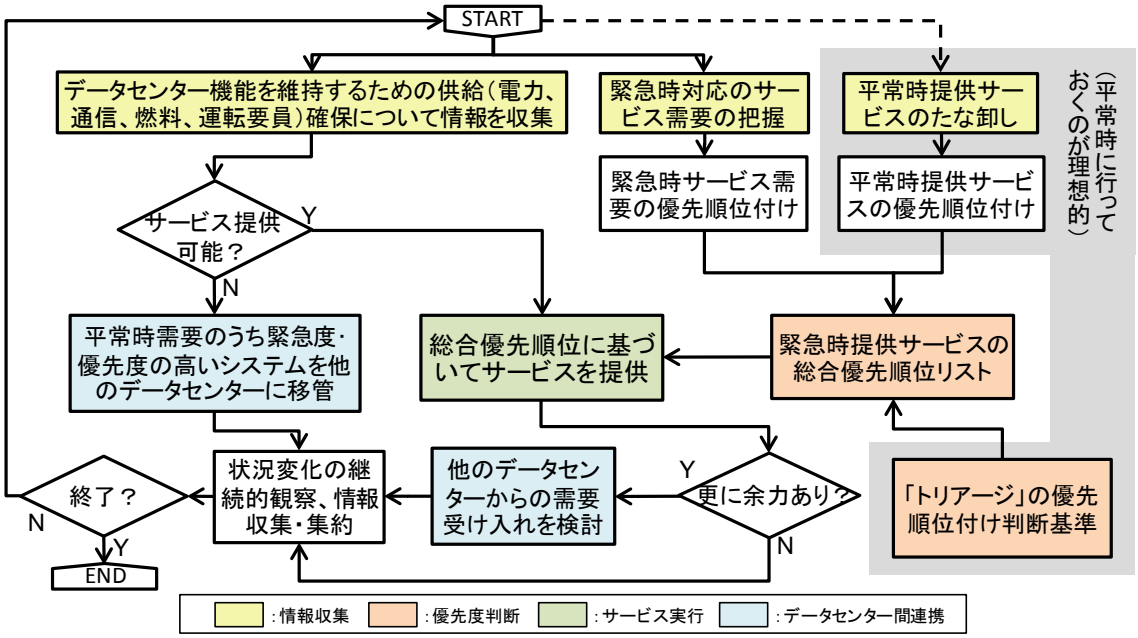


緊急時にリソースの供給サイドの情報を把握してクラウドサービスの供給可能量を量り、また緊急時対応を含む需要側の量を把握して、予め決めておいたプロセスと判断基準に基づく優先順位付けを行いながら、リソースの配分を行うプロセスである。

データセンターの機能がどの程度維持・提供できるのか、の供給サイドの判断と、緊急対応や重要インフラの機能維持のために緊急に必要とされるシステムニーズの把握、ならびに、そのデータセンターが平常時に担っているサービスとの優先度に関する、需要サイドの判断の両方を、平行して行わなければならない。

この情報収集と判断のプロセス(「トリアージ」)は、一例として、図表 98 のように表わせる。

図表 102 クラウドの「トリアージ」の判断プロセス・フローの例



この例では、トリアージの考え方に基づき、平常時においてそのデータセンターが提供しているサービスのリストが把握されており、かつその間の優先順位付けも行われていることを想定している。緊急事態が発生したときは、1)データセンター機能を維持するための供給(電力、通信、燃料、運転要員)確保について情報を収集するとともに、2)緊急時対応のために発生する IT サービスに対する需要の把握を行う。

次に、緊急時需要について優先順位付けを行う。この際も、予め設定された判断基準に基づき行うことが、混乱を避け迅速性と効率性を担保するために必要である。この順位付けられたリストと予め優先順位付けられた平常時のサービスリストをマージして、総合優先順位リストを作成する。このために判断基準も予め定めておく必要がある。一例として、以下のような優先順位付けが用意されているとよいのではないかと考えられる。

1. 人命・生命の維持に関すること（救急、緊急医療、飲食料の供給）
2. 緊急支援・緊急対応に直接関すること（避難生活を支える情報管理、救援物資配給）
3. 重要インフラ等社会基盤のうち重要性の高いシステム（ライフライン、物流、金融）
4. 緊急支援・緊急対応に二次的に関すること（地域行政対応、避難者の心身ケア、支援者のサポート）
5. 企業の生産活動に関するもの（在庫のない生活必需品、サプライチェーンの長い工業品）
6. 都道府県・国レベルの広域行政対応（通常システムでまかないきれない部分）

（ただし、1～3 の順位は状況に応じて変える）

データセンターを稼動させるために利用可能なリソースの把握が行われると、サービスの供給が可能か、どの程度サービスを提供できるかの情報が得られる。サービス提供が可能であれば、その能力に応じて、需要側の優先順位リストに対して、順次サービスを提供する。

もしそのデータセンターの能力が需要に対して十分大きく、余裕がある場合には、他のデータセンターで対応できない需要を引き受けることも検討されるべきである。

また逆に、当該データセンターのサービス提供が不可能な場合や、重要度の極めて高い需要を満たすには能力不足であるような場合は、当該データセンターが抱える優先度の高い需要を他のデータセンターに振り向けることを行わなければならない。

災害時等には、状況は刻々と変化するので、一定時間のインターバルで、あるいは状況に大きな変化が生じる都度、この判断サイクルをまわす必要がある。

この考え方で重要なのは、、予め判断プロセスのフローと基準を用意しておくことである。事態が発生したときに現場において用意するべきものとしておくと、緊急事態で情報と状況が錯綜する中で、体系だった判断が困難になり、不適切な判断基準や矛盾した、あるいは首尾一貫性のない判断に陥りがちである。したがって、平時において基本枠組みを定めておく必要がある。それによって初めて、いざというときに実際の現場で起こる不確定要素を、予め定めた枠組みに組み込みながら、的確な判断が実施できるようになる。

逆に、緊急時における発生事象を考えうる限り想定し、その組合せを幾通りも用意して、各々に対して最適解を設計しておく考え方は、緻密な計画のようでいて、いざというときに機能しない恐れがある。なぜなら、非常時に生起することは平常時の想定どおりにいかないことが多い上、余りに精緻で複雑に分岐した状況想定では、適用条件の照合に手間を取られ、細部の相違を吸収するための応用問題に頭を悩ますことになり、効率を著しく阻害する恐れが強いからである。

個別状況でなく判断プロセスと判断基準を整備することにより、緊急時にクラウドがその

機能を維持し、あるいは早期に回復し、緊急対応のために必要なサービスを、優先順位をつけながら供給し、社会インフラとして機能することが期待される。

より具体的には、図表 99 に示すようなフレームワークを用意し、これに沿って準備を行った上で、緊急時対応にも活かすといったことが考えられる。クラウドのレジリエンシのための「トリアージ」的アプローチにおける考え方や判断ポイントの一例として示す。

図表 99 クラウドのレジリエンシのための「トリアージ」的考え方・判断ポイントの例

データセンター	内訳項目	前提となる平時の準備	緊急時対応の考え方		
			基本	バリエーション	備考
電力	通常商用電力 ＜コンピュータ電源＞ ＜コンピュータ室空調用電源＞ ＜オペレータ室電源＞	供給系統の二重化（ただし広域停電時には役に立たない）	電力源確保を最優先に対応	緊急時にコンピュータ室内でのオペレーションに移行する代替策も	電力会社の復旧見通し公表が重要
	UPS	電力の瞬断・瞬低対策と、停電時の予備電源への切り替えのつなぎ目的であり、代替電源と位置づけない。	電源切り替え時の短時間の代替補償であり、補完的役割以上のものを期待しない		
	非常用発電機	・予備電源・自家発電装置の設置 ・定期点検により、いつでも稼動できる状態を維持	商用電源喪失時に自動起動・自動切換え実施	給電範囲を細かく区分	長時間連続運転に耐えないことを考慮
	非常用発電機燃料	・適法の範囲で最大量の備蓄 ・近隣への二次備蓄の検討（輸送手段含む）	備蓄補充の手配を行う		
		非常用発電機のための燃料補給契約：優先供給契約および契約先の二重化	定期的供給・補充を確保する	二次補給源を用意することも視野に	
ガス	非常用発電機燃料	・耐震性の確保 ・複数供給ルートの確保 ・LPGの貯蔵を選択肢として持つ	LPGを燃料とする場合、LPGの定期的供給・補充を確保する		地震被害の場合都市ガスの供給は当てにならない？
	非常時運転（泊り込み）要員の生活熱源	カセットコンロ・ボンベの備蓄	必要に応じて運転要員に提供	必要に応じ、店頭または救援源から追加調達	
水道	コンピュータ室空調用冷却水	・一定時間空調を維持できるだけの冷却水の備蓄 ・水冷を避け空冷を選択する考えもある。	・備蓄補充の手配を行う ・冷却水を補給せずに運転可能な時間の把握		
		一部空冷にして冷却水不足をヘッジする方法もある。	冷却水なしで運転できる範囲（稼動させるシステム）を決める		
	非常用発電機用冷却水	一定時間運転継続できるだけの備蓄	非常用発電機の運転ニーズに合わせて供給		冷却水の補充を必要としない予備電源の設置が基本
	トイレ用水	・貯水槽等での対応 ・簡易トイレ等の備蓄	必要に応じて運転要員に提供		近隣施設の利用も
通信回線	常用データ通信回線	通信回線の冗長化	・通信回線確保は電源に次ぐ優先確保項目 ・利用の優先付けに対応した選択・運用		
		複数通信事業者との契約			
		複数中継局との接続			実現可能性チェック
	非常時の縮退運転用データ通信回線	無線通信手段の確保	・中継局の死活に応じた使い分け ・バッテリ容量を考慮	バッテリ充電電源の確保	暗号化への考慮
		衛星通信手段の確保	・連絡・業務のための予備通信手段 ・原則としてサービス提供手段としては利用しない		
	非常時の連絡用通信手段	・携帯電話（3G+LTE） ・衛星電話 ・データ通信用モデム	・中継局の死活に応じた使い分け ・バッテリ容量を考慮		
運転・保守要員	非常時シフト（泊り込み含む）編成	・複数のバリエーションによる班・シフト編成 ・非常時召集（安否確認含む）の定期的訓練	緊急対応計画に基づく召集・シフト体制の発令	出勤・帰宅困難者の状況に応じてシフト編成を臨機に変更	
	泊り込み要員のための生活備蓄（水、食料、寝具、トイレ、熱源）	・必要量の想定（人数×想定日数） ・備蓄品の消費期限の管理 ・備蓄場所の選定と周知、鍵管理	必要に応じて運転要員に提供	・必要に応じ、店頭または救援源から追加調達 ・余裕がある場合、避難民への提供を考慮	
	通勤・交通手段	・組織として、各要員の常用交通手段、迂回・代替交通手段の把握 ・徒歩ルートの確認と実況検分	・通勤経路の利用可能性・安全把握 ・危険のない範囲で出勤できる要員を優先確保	データセンターから徒歩圏内で住宅を確保することも検討対象	
コンピュータシステム	常用システム	・信頼性に関する評価（自己評価、第三者評価） ・経産省「情報システムの信頼性向上に関するガイドライン」、同「情報システムの信頼性向上に関する評価指標」、IPA「信頼性自己診断ツール」の活用	・電源容量、運転要員量に応じて縮退。 ・アプリケーション（用途）に基づく優先選択		
	HA構成	冗長化構成、常用予備切り替え機能の確保	主システムの停止に伴い自動起動･自動切換え		
	システム・バックアップ	・設定の保存 ・マシンイメージの保存 ・リストア作業手順の作成・周知徹底と定期的訓練	コールドスタンバイシステムの場合、リストアを実施		
確保すべきサービスの選択	常用系の重要システム		・重要インフラを中心に非常時に確保すべき機能を確保 ・緊急対応の高優先事項との比較で、優先度の低いサービスを抑制		
	非常時対応のために緊急に必要なシステム･サービス		以下のものを第一優先と位置づける。 ①救援・救急の中核システム ②救援・復旧物資の集荷・物流・配備のための基幹システム ③被災者管理の情報システム ④行政の非常時対応のための基幹システム ⑤被災者への医療・医薬等供給のための情報システム	住民の把握、移動把握、状態把握のためのシステムを第二次優先で用意する。 時系列で追随できる機能や、情報をタイムリーに定常的に吸い上げられる機構も併せて整える。	
利用主体（緊急時データセンターサービスの受益者）の選択	非常時対応・緊急対応の主体		以下のものを第一優先と位置づける。 ①市区町村 ②市町村の出先機関 ③都道府県・政令指定都市 ④被災者支援のボランティア組織	現場判断が困難な場合、国や都道府県の指示を仰ぐ可能性も考慮	国は別途独自に非常対応機能を確保することを前提とし、支援対象の優先順位には含めないこととする
	被災主体または緊急対応の副次主体		以下のものを第二優先と位置づける。 ①被災者 ②被災企業 ③支援企業		
	重要インフラおよび重要インフラを支える二次供給系		重要インフラは第一優先の対象となるが、多くが独自のシステムを持って運用している実態から、別途、要請に応じて対応する。 対象としては、電力、通信、水道、ガス、物流、金融が中心となる。	重要インフラに準じるものとして、非常用電源の燃料の供給事業者（石油製造・流通事業者）を優先対応対象とする。	現場判断が困難な場合、国や都道府県の指示を仰ぐ可能性も考慮

3.3. 個別の取り組みで満たすべき要件

今まで述べたような基本的な考え方に基づくと、クラウド事業者や社会全体で満たすべき具体的な要件は、次の図表 102 のように整理される。

図表 103　事業継続の観点からのクラウド事業者等が満たすべき要件

項目	要件	関連する事例、有識者からの指摘等
平常時からのファシリティ面の対策	• 3.11 前から講じられてきた堅牢性を確保するファシリティ基準の継続的な遵守 • 津波・液状化をはじめ、3.11 前に想定が弱かった対策の強化	• 3.11 時にデータセンターはほとんど無傷で、事業継続できた。もっとも、件数は少ないものの、サーバ室の天井が剥がれ落ちたケースと免震構造のサーバーキャビネットが倒れたケースが見られた。これらはこれまで想定していなかったため、ハード面の基準として見直す必要がある。 • 液状化の影響は 3.11 前までは、十分考慮したデータセンターのファシリティ基準となっていなかった。津波への対策も同様である。これらについて、対策を強化する必要がある。
平常時におけるライフラインの冗長性確保	• 電力・通信等のバックアップ手段確保	• 電力の復旧に時間を要したほか、計画停電もおこなわれた。ライフラインに対する準備が平常時から重要であった。 • また、現状では通信回路が単一であるところが緊急・災害時には問題となる可能性がある。とはいっても、エンドユーザに対してはコスト等の関係で推奨するに留まらざるを得ない。
緊急・災害時における代替ライフラインの確保		• 緊急・災害時には通信回路の確保に加えて、その容量も問題となりえる。 • 非常用の自家発電機は耐用時間が短く、長期間の停電には耐えられない。
緊急・災害時における代替ライフライン確保のための二次的サプライの要件	• 緊急・災害時の燃料等の社会全体での最適配分の仕組みづくり	• 非常用電源を動かすための燃料が重要である。データセンターは備蓄と補給でなんとか稼働し続けたが、一部銀行の電算センターでは 3 時間程度の燃料備蓄しかなく、停止した。 • 燃料の優先供給契約は 3.11 ではほとんど機能しなかった（タンクローリーの不足、交通遮断、被災地への優先的供給など）。 • 燃料供給者の視点からは、要望が殺到する中で優先順位を付けて供給することは民間では無理がある。公的な指示が必要。
データセンターの運転ならびに保安のための要員に関する	• 緊急・災害時において少ない要員での稼働、ないし要員参集を前提としない稼働に向けた準備	• 3.11 は金曜の昼間であったから深刻な問題とならなかったものの、夜間の場合であったら要員確保は懸念される。 • 交通寸断により要員確保が難しくなるケース

項目	要件	関連する事例、有識者からの指摘等
要件		も想定される。 • 3.11 のときは大きな問題とならなかったが、大規模な自然災害の後にインフルエンザなどの感染症が広がるリスクもある。
緊急・災害時におけるセキュリティ対策、ならびに意図を持って行われるサイバー攻撃に対する防衛または回避	• 緊急・災害時の状況に応じたセキュリティ基準緩和の手続き、監査・監視に向けた準備 • サイバー攻撃等に備えた対策の厳格な運用	• 緊急・災害時には厳重なセキュリティチェックが難しくなるケースがある。たとえば、電力補給のためにデータセンターへの入館を比較的容易に認めるといったケースも想定される。 • 医療における患者のデータ共有がクラウドで円滑に進むと、災害時の人命救助等の点で効果的である。ただし、その際の個人情報保護を含めたセキュリティ対策をどこまで緩めるのか、また誰がどのような手順でセキュリティを監査・監視するのかという課題は残る。 • クラウドにおいてもサイバー攻撃等に備えた対策としての基本的な事項は、通常の IT の場合と同様である（アクセス制限をかけることやデータの暗号化を進めることなど）が、クラウド化すると攻撃を受けうる対象が増えるため、より厳格な対策が必要とされる。
その他	• 契約におけるトラブル対策の責任の所在、手続きの明確化 • 中小事業者等のサービス途絶リスクに対する社会としてのセイフティネットの構築	• 南海トラフ地震など、現状の BCP で想定している以上の災害リスクにどのように対応すべきか。 • 平常時、緊急・災害時を問わず、クラウド事業者が倒産したり、トラブルが起きたりした際の責任の所在を明確にしておく必要がある。

III. システムやベンダーの枠を越えたデータセンター間連携やクラウド間マイグレーションを可能にするために必要な諸要素の調査

1. 問題認識

クラウド事業者間連携に関する欧米と日本の問題認識の違いに触れながら、日本としてクラウド事業者間連携に対してどう取り組むべきかを検討する。なお、クラウド事業者間連携の実現に必要な要素としてクラウドの標準化があり、クラウド標準化も含めた形で動向を整理する。

1.1. 欧米の動向

欧米においては、米国国立標準技術研究所（NIST）、Distributed Management Task Force（DMTF）、Open Data Center Alliance(ODCA)等の標準化機関や業界団体がクラウドの標準化やクラウド事業者間連携に関するフレームワークを議論し、積極的に進めようとしている。しかしながら Amazon、Google などの大手クラウド事業者側は、ユーザ企業が他クラウド事業者サービスに取り込まれるのを避けるべく、独自仕様を実装し、自社サービスから簡単に他サービスへ移行できないようにするために、標準化には消極的であるとの見方もある。また自社で複数データセンターにクラウドサービスを展開し、かつデータセンター間の連携ができていることから、事業者間連携に対する意識はない。このことから、クラウドの供給サイドにおいては、クラウド標準化、クラウド事業者間連携に関する議論は進んでいない状況であると言える。

一方、ユーザ企業は、クラウド事業者から囲い込まれることなく、むしろクラウド事業者をコントロールできるように、自らクラウドサービスおよびクラウド技術に関するリテラシー（正しい理解と使いこなす能力）を高め、クラウドサービスをうまく組み合わせたサービスモデルやベストプラクティスを議論する傾向にある。たとえば、ODCA に UBS（スイスの大手銀行）、ドイツ銀行、BMW（ドイツの高級自動車メーカ）等のユーザ企業が参加し、クラウド標準化、クラウド事業者連携に関するフレームワークを議論していることから、その一端は覗える。

また、そのようなクラウドサービスをマッシュアップ的に組み合わせるサービスを提供するクラウドブローカービジネスも出てきている。NIST[80]によるとクラウドブローカーは以下の 3 つに定義される。

1. Service Intermediation（クラウドサービスの仲介）

クラウド事業者が提供するサービスに対して、特定の機能を改良したり付加価値を付け加えたりして強化したサービスを、クラウド利用者に提供する。改良項目としては、クラウドサービスへのアクセス管理、ID 管理、性能レポート、セキュリティの強化などがある。

[80] NIST SP800-292 Cloud Computing Reference Architecture による

2. Service Aggregation（クラウドサービスの統合）

1つまたは複数のクラウドサービスを組み合わせることにより、新たなクラウドサービスを利用者に提供する。その際、クラウドブローカーは、データの統合や利用者と複数のクラウド･プロバイダー間の安全なデータ転送を提供する。

3. Service Arbitrage（クラウドサービスの裁定取引）

「クラウドサービスの裁定取引」は「クラウドサービスの統合」と似ているが、違いは「クラウドサービスの裁定取引」の方が、集約するサービスを固定していない点である。つまり、クラウドブローカーが複数のクラウドサービスから選択する柔軟性を持っていることを意味する。例えば、スコアリングサービスを使ってクラウドサービスを評価し、最高の評価を持つサービスを選択するといったことを行う。

1.～3.において共通するブローカーの主な提供機能としては、「セルフサービスの契約手続きおよびプロビジョニング」「複数サービスにまたがるアクセスコントロール」「SLA に応じたパフォーマンス監視」「利用状況に応じた料金算出と課金処理」「ヘルプデスク」など、ユーザが利用したい機能をひとまとめに用意しているのが特徴である。このような機能はクラウドサービス側の API を通じて提供できるようになっており、ユーザから実際に利用するクラウドサービス仕様が見えるようにしている。また、重要なデータについてはクラウドサービス側で保存される。

ただし、1.～3.全体において、ブローカーは複数のクラウドサービス利用の入り口を一つにしているが、クラウドサービスの機能を組み合わせたり、あるクラウドサービスが停止した場合に他クラウドサービスにリソースを移してサービス継続性を図る BCP の要素は含まれていない。

背景として、欧米においては、ユーザ企業自らクラウドに対するリテラシーを身につけ、クラウドサービス毎の機能、価格、可用性、既存システムとの連携を吟味し、リスクがある部分については、複数のクラウドサービスを利用することで、クラウドサービス事業者の冗長化を図り、クラウド導入後、よりよいサービスが出てくれば柔軟にクラウド事業者を乗り換えていくなど、クラウドサービスの継続性を自ら確保するという共通理解ができつつあるのではないかと考えられる。また、そのようなユーザニーズを受けて、クラウドサービスを組み合わせる手助けとなるべく、クラウドブローカービジネスが今台頭してきているのではないかと推測できる。

1.2. 日本の動向

日本においては、グローバルクラウド基盤連携技術フォーラム（GICTF）がクラウド事業者間連携について、積極的にユースケースを規定し、標準化を進めるべく活動している。その考え方は、広範囲にわたる大規模災害やデータセンター内設備等の大規模故障が

発生した際に、ユーザ企業に対してクラウド事業者がサービスを継続させるためにクラウド間連携を実施する状況を想定し、クラウド間の監視・死活の確認、代替リソースの発見・確保、リソース管理やサービスセットアップ及びサービスのマイグレーション、認証連携等の要件について検討し共通認識やインターフェイスを形成しようとするものであり、DMTF など標準化団体に働きかけて国際的な標準としての開発を目指している。

ただし、現状では、国内の大手クラウド事業者側は、欧米同様、自社サービスにユーザ企業を囲い込めないこともあり、あまり積極的ではない状況がうかがえる。

ユーザ企業の動きとしては、欧米と違いユーザ自らというよりは、今までの IT パートナーであるシステムインテグレータに、初期導入におけるクラウド事業者の選定や、場合によっては複数クラウドサービスの機能連携、ユーザの既存システムとの連携の実現を依存する傾向にある。さらに、クラウドサービス側でトラブルが発生した場合はその対応責任をもシステムインテグレータに負担させるケースが多い。

システムインテグレータがこのように複数クラウド事業者を束ねる点については、欧米のクラウドブローカーに似ているといえる。しかしながら、システムインテグレータは単純な仲介ではなく、複数のクラウドサービス機能を連携させて新たなクラウドサービスとして提供している点がクラウドブローカーと異なっている。また、ユーザに対してクラウドサービス仕様を直接見せずに、システムインテグレータのサービスとして見せている点ででも違いがある。

クラウド事業者側のインタビューの中では、事業者間連携に対して否定的な意見が多く見られた。しかしながら実際には事例や証言を総合してみると、国内のクラウド事業者においては、規模に関係なく事業者間連携に対するニーズがあった。

その第一は他の事業者へのリソース提供である。たとえば、中小のクラウド事業者が一時的な需要増への対応として大手クラウド事業者のリソースを借りたいというニーズがあるという。第二は自社のクラウド事業の差別化要因として、事業者間連携サービスを提供している事業者がある。第三には大手クラウド事業者の中にもクラウドサービスの DR サイトを用意しているものの、収支面からメインサイトと同じリソースを DR サイトでは準備できないため、状況によっては他の事業者が保有するクラウドサービスからリソースを借り受けたいというものである。

以上をまとめると、日本におけるクラウド間連携に対するニーズには以下のような特徴があることがわかった。

まず、東日本大震災に見るように災害が多い国であり、欧米と比較してクラウド事業者間連携の必要度は高い。また、ユーザ企業はクラウドとの連携を含めたシステム全体の継続性確保をシステムインテグレータに求め、システムインテグレータは自社のサービスの一部としてクラウドサービスを提供する傾向にある。一方、クラウド事業者側の自身の事業継続性において全てがしっかり準備できているとは限らず、ユーザはもとより、システムインテグレータもその事に気付いているのか疑問が残る。

したがって、クラウド事業者にとっては自身の事業継続性の観点からも、まずはクラウド事業者、システムインテグレータ双方が、クラウド事業者間連携に関する議論を深め、国内ユーザに発信し、ひいては日本から世界に発信することが望ましい。

2. 現状の取り組みと課題

2.1. 事業者の認識

いくつかのクラウド事業者に、クラウド事業者間連携への取り組み状況について、インタビューした結果、「積極的に取り組んではいない」事業者と「関心はあるがアイデアの域から出ない」事業者の 2 つに分かれた。

積極的ではない理由としては、主に「自社で複数サイトを持っており、他社と連携の必要がない」という理由だった。また、アイデアの域から出ない理由としては、下記のようないくつかの問題点が挙げられた。

- 事業者ごとのセキュリティポリシーや SLA の差異をどうするか。
- クラウド事業者間の契約形態をどうするか。
- 重要データを扱うシステムほど、再委託を嫌がる点をどうするか。
- 仮想化環境の差異を吸収できるか。
- 仮想マシンイメージ移行をネットワーク越しでやる場合は、回線帯域、遅延の影響を考える必要がある。
- クラウドをまたがるデータコピーは事前に準備しておかないと、転送に時間を要する。

2.2. 先行的な取り組み事例

上記の通り、異なるクラウド事業者間連携に関して、否定的な見方が多い。しかし、広域災害を想定してサービス継続を実現するために、事業者間連携を行うという考え方が出てきている。以下に、国内ではまだ少数と考えられる、事業者をまたいだクラウド間の連携事例を紹介する。前述したとおり、他社との連携を必要としているクラウド事業者は存在するため、今後も取り組み事例が増えてくるものと想定される。

2.2.1. 取り組みの背景

東日本大震災とその後の電力の供給状況を踏まえると、配電系統が異なっていたとしても同一電力事業者の管内では電力の完全な安定供給は保障されないとの判断の下、電力事業者の枠を越えた場所での災害復旧サービスを行うことが望まれた。また、ユーザから「30 メートルの津波がきたら大丈夫か」と聞かれるようになり、データセンター事業者として選択され続けるには、1 社における堅牢性の追求では限界があり、地方のデータセンター事業者として全国にアピールするために、連携を行うことを決断したという。

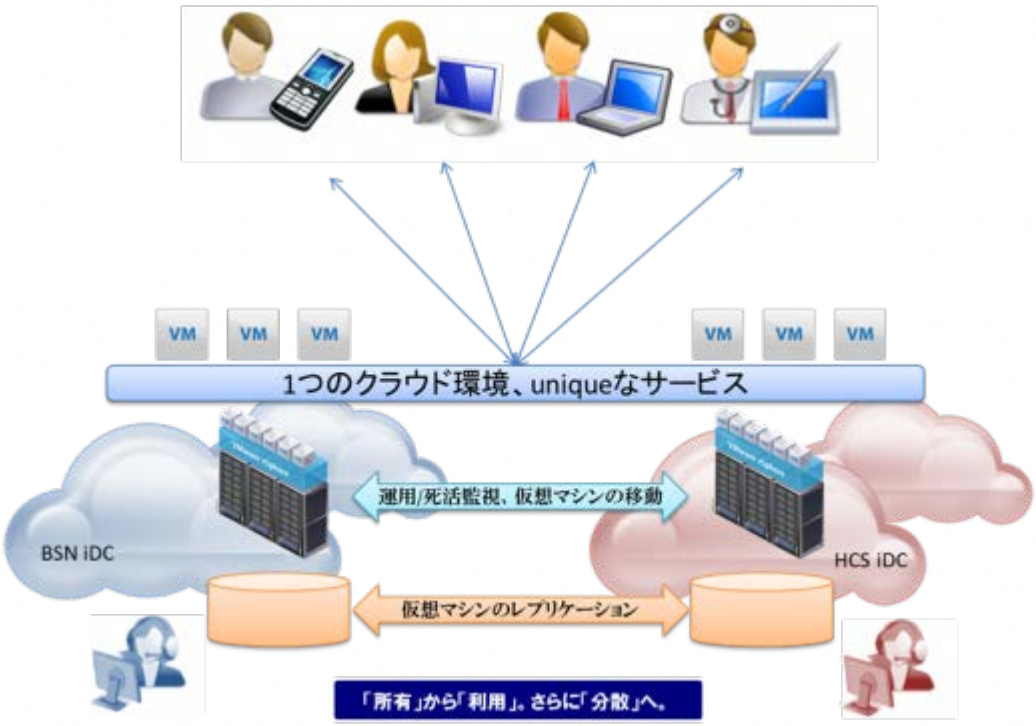
2.2.2. 取り組みの内容

新潟市の BSN アイネットと富山市の北陸コンピュータ・サービスは 2012 年 3 月 5 日、VMware 社のソリューション、vCenter Service Recovery Manager（SRM）を使った災害復旧（DR）サービスを提供開始したと発表した。異なる事業者が SRM で連携し、DR サービスを双方向で提供するのは、これがおそらく国内では初めてと考えられる。先に述べた電力事業者の管轄は、BSN アイネットが東北電力（周波数 50Hz）、北陸コンピュータ・サービスが北陸電力（周波数 60Hz）と、異なる電力会社の供給区域にあるため、大規模な停電、計画停電の影響を受けにくいと考えられる。

データセンター間の距離は 200km。単一の災害で同時に被災する、少なくとも同時に機能停止に陥る可能性が極めて小さい距離である。このサービスの 1 つのポイントは、データセンター間で対称的なシステムとなっており、各機種を同一にしている。復旧時間のめどは 30 分で、復旧状態を顧客に確認してもらう。

この事業者間連携の上に乗って運用されているシステムの例としては、歯科医院向けレセプトシステム、公立病院向け経営分析・財務会計システム、自治体向け財務会計業務システム、ガス上下水道料金・公営企業会計、総合行政情報ネットワーク、民間向け販売システムがある。 重要インフラに該当するシステムが多く乗っている点が注目される。

図表 101 クラウド基盤連携サービスのイメージ



出所）株式会社BSNアイネット、北陸コンピュータ・サービス株式会社ニュースリリース（2012 年 3 月 5 日）
http://www.bsnnet.co.jp/news/news20120305/（2012 年 6 月現在）

この事例は、大手事業者にはない、地域に密着した中堅事業者ならではの取り組みとして注目される。今後、地方自治体などのシステムを預かる地方中堅事業者が大手の進出に対抗するビジネス上の要求からも取り組みが増えていくことが期待される。

3. クラウド間連携等の実現に向けた諸要素

本節では、クラウド間の連携の実現に向け、解決が必要となる課題を技術および制度の面から検討を行った。その概要は以下の通り。

3.1. クラウド間連携がスムーズに実現するための技術的要件

3.1.1. 検討の進め方

異なるプラットフォーム間で、仮想マシンインスタンスもしくは仮想マシンモニタのレイヤーで移行・移転（いわゆるフェイルオーバまたはマイグレーション）をスムーズに実現するために必要な技術的要件について、NIST の定義や各標準化団体で規定している共通仕様、有識者・クラウド事業者へのインタビュー結果などを元に検討を進める。

3.1.2. 各標準化団体で規定している共通仕様

クラウド間連携に必要な技術的要件を洗い出す前に、クラウド間連携視点で、各標準化団体で規定している共通仕様のうち、主だったものについて触れていく。（略称のフルスペル等は図表 101 参照）

(1) DMTF の OVF

仮想マシン（VM）のディスクイメージの標準フォーマットである OVF（Open Virtualization Format）を DMTF にて策定。仮想マシンイメージのポータビリティを考える上で、現在非常に利用されている共通フォーマットである。

(2) SNIA の CDMI

データパスだけでなく、クラウド環境に保存されたデータに対するサービスレベル管理、データ移動や関連データとのやり取りにおける共通フォーマットなどを定義。保存するコンテンツのメタデータを保持するように設計されている。これにより、異なるクラウド間にて、ストレージの機種や様々なファイルシステム（NFS、CIFS、WebDAV など）を意識せずに、CDMI で規定している API 経由でデータの移動が可能となる。ただ、EMC や日立など主だったストレージベンダからの対応製品の提供はほとんどなく、まだ普及はしていない模様である。

(3) OGF の OCCI

2009 年にOGF内で立ち上がったOCCI-WGにて、IaaS管理用インターフェイスAPIの

共通仕様となるOCCIを策定。RESTful API[81]に準拠していることが特徴で、プロビジョニング等のIaaS管理が遠隔から可能である。「OpenNebula[82]」、「OpenStack[83]」など主要なオープンソースのクラウド基盤構築ソフトに実装されている。

主要な標準化団体とその提唱する共通仕様を図表 103 にまとめた。

図表 104 クラウドに関する標準化団体一覧

団体名	概要	共通仕様
OGF (Open Grid Forum)	1999 年設立、400 以上の機関が参加。 Open Cloud Computing Interface Working Group (OCCI-WG)においてクラウドコンピューティングインフラの遠隔管理を可能とする API を検討	IaaS の管理インターフェイス API である OCCI（Open Cloud Computing Interface）を策定
DMTF (Distributed Management Task Force, Inc.)	企業やインターネットにおける IT 環境のシステム管理のための標準を策定・保守する標準化団体。1992 年設立。43 カ国以上から 160 以上の機関が参加。クラウド基盤上にアプリケーションを実装するための規約策定に向け、2010 年に作業チーム Open Cloud Standards Incubator により 白書を作成、その実現に向けた活動	IaaS の管理インターフェイス API である CIMI（Cloud Infrastructure Management Interface）を策定 VM のディスクイメージの標準フォーマットである OVF（Open Virtualization Format）を策定
SNIA (Storage Networking Industry Association)	1997 年 12 月設立、参加社数 250 以上 クラウドとのデータ読み書きに関するインターフェイス CDMI（Cloud Data Management Interface）の策定とその導入に向けた活動である Cloud Storage Initiative を運営	クラウド管理インターフェイス仕様（CDMI）を策定
OASIS (Organization for the Advancement of Structured Information Standards)	1993 年に SAML Open として発足（1998 年に OASIS に改称）100 カ国以上から 600 以上の機関が参加。 クラウド上の ID 管理・相互運用性の課題検討のための技術委員会を設立	IDCloud TOSCA
Open ID Foundation/ Kantara Initiative	2007 年設立。著作権管理、商標管理、仕様を自由に使うことができるようにするための標準化プロセスの管理、OpenID 財団の標準化プロセスで標準化された各種規格についての普及啓蒙を実施。	次世代の認証・連合アイデンティティシステムの標準である「OpenID Connect」を策定 クラウドサービスにおけるアイデンティティ・プロビジョニング・インタフェースの共通仕様（SCIM（Simple Cloud Identity Management））を策定
OMG (Object Management Group)	1989 年設立、参加社・機関数数百。組み込みソフトからビジネスアーキテクチャーなど幅広い分野の標準化団体。2011 年 4 月にクラウド導入に向けたアドボカシーグループ Cloud Standards Customer Council を設立。多様なクラウドインフラ上のアプリケーションのモデル化などを検討。	—
TCG (Trusted Computing	トラステッドコンピューティングを実現するためのオープンスタンダードの検討、策定そしてその普及を促進するための非営利団体。	プラットフォームの正当性証明機能、データの暗号化機能、電子鍵および電子証明書の安全な保管機能などを提供するオン

81 2000 年に Roy Fielding 氏が提唱した、分散システムにおいて複数のソフトウェアを連携させるのに適した設計原則を Web に適用したソフトウェアの設計様式に基づいて作成されたアプリケーションインターフェイス。パラメータを指定して特定の URL に HTTP でアクセスすると、XML で記述されたメッセージが送られてくるような呼び出しインターフェイスである。

82 2008 年 3 月に OpenNebula Community によって初版がリリースされたオープンソースの IaaS 構築ソフトウェア。

83 Rackspace Cloud 社と NASA（米国航空宇宙局）の共同プロジェクトで開発され、2010 年 10 月に初版がリリースされたオープンソースの IaaS 構築ソフトウェア。

Group)		ボードチップである TPM(Trusted Platform Module)の規格を策定
GICTF（グローバルクラウド基盤連携技術フォーラム）	2009 年設立。クラウドシステム利用技術等の開発・標準化の推進を目的に、クラウドシステム間連携を実現する標準インターフェイスの提案を行っている我が国の団体。2007 年 7 月に米 DMTF と提携した。	―

3.1.3. 基本的な考え方

ユースケースとして、広範囲にわたる大規模災害やデータセンター内設備等の大規模故障が発生した際に、ユーザ企業に対してクラウド事業者がサービスを継続させるためにクラウド間連携を実施する場合を想定する。

その場合、クラウド間連携を実現させるための技術的な方式は、以下の 2 つに大別されると考えられる。

① 大規模災害発生時に、連携先クラウドサービス内のリソース調整（発見・確保）を行い、仮想マシンおよびデータを移行させる。

② 予め、連携先クラウドサービスの仮想マシン、ストレージ、NW におけるリソースを確保しておき、平常時に定期的にデータ同期を実施。

これまでの調査結果から、クラウド上で運用するシステムの規模が大きくなればなるほど、大規模災害が発生してから他クラウドサービスに仮想マシンを移行させるのは、不確定要素がいくつかあり、RTO/RPO[84]を守ることが難しく、現実的ではないと考えられる。具体的な不確定要素は以下の通り。

- 移行先リソースの発見・確保が想定通りの時間でできるか
- 仮想マシンイメージをネットワーク越しに転送するのは、その時の回線状況に依存するため、想定通りに行かない場合も考えられる
- データ領域を移行させる場合は、ストレージ間コピーが有効だが、各サイトのストレージが異機種であるとコピーが難しい場合がある。
- 通常ストレージは内部の管理ネットワーク上に配置されているため、ストレージ間をつなぐ場合はネットワークセキュリティを予め考慮に入れておく必要がある。

それよりも、平常時に連携元クラウドサービスと連携先クラウドサービスの双方に必要な仮想マシン、ストレージ領域、回線帯域を確保しておき、一定の間隔で両サービス間のデータ同期を実施し、大規模災害発生に備えておく方が、予め決められた RTO/RPO を守ることが可能であり、特に重要インフラ・業務における事業継続を前提とする場合は、この②の方式が妥当だと考える。以下では②の方式をベースに、クラウド間連携がスムーズに

84 RTO:Recovery Time Objective（復旧目標時間）障害発生前の状態に回復するまでに許容される時間。システム停止が許容される時間。
RPO:Recovery Point Objective（復旧目標地点）障害発生前の「いつ」の状態に復旧するかという目標。RPO 以降障害発生までのデータ等は復旧できないため、失われるデータ等の許容される範囲を定めることとなる。

実現するための技術的要件について述べる。

3.1.4. 具体的な技術要件

前項の②の方式を前提におき、具体的な技術要件についてまとめる。検討対象として、単一の IaaS における主な構成要素である、「リソース」、「サービスマネジメント」、「セキュリティ」について、以下の要素を取り上げた。

＜リソース＞

・クライアント向け回線（インターネットなど）

・仮想マシン

・ハイパーバイザー

・ネットワーク（LAN）

・ストレージ

＜サービスマネジメント＞

・運用

・セキュリティ

また、クラウド事業者間連携に必要な要件として、「ポータビリティ」、「相互運用性」が挙げられる[85]。これらの組合せによる技術的要件は図表 104 のようにまとめられる。

図表 105 クラウド間連携実現のための具体的な技術要件

クラウド単体の構成要素	クラウド間連携に必要な要素	
	ポータビリティ	相互運用性（プロビジョニング含む）
クライアント向けネットワーク（インター ネットなど）	—	• 災害時、利用者から他のクラウドサービスへのアクセスが動的に切り替わること • 災害復旧時、利用者が元のクラウドサービスにアクセスできるよう動的に切り戻ること
サーバ（仮想化技術）	• クラウドサービス間の仮想化環境の差異を吸収すべく、OVF のような標準化されたフォーマット及びインターフェイスを用いること	• 連携元クラウドサービスから連携先クラウド事業者へサービス提供に必要なリソースの構成情報とサービスのデータを、自律的に転送できること • 連携元クラウドサービスにて、上記リソースの構成情報とサービスのデータの更新が発生した際は、適宜差分を連携先クラウドサービスへ自律的に転送できること
ネットワーク	• クラウドサービス間で仮想マシンの移行ができるよう、プライベートアドレスが重複しないようにすること • プライベートアドレスが重複する場合でも、中間で IP アドレス変換するなど、問題なくクラウドサービス間でルーティングができ、移行先に問題なく、仮想マシンイメージ	• 異なるクラウド事業者間で、ストレージ内データ、仮想マシンデータをスムーズに移行できるよう、遅延を考慮した回線帯域を、クラウドサービス事業の成長に合わせ、双方の事業者で随時検討すること • クラウドサービス間通信において、圧縮技術等を用いて、データ通信時間を短縮すること • クラウドサービス間にてある程度大容量のデータ転送が発生する。ネットワークの負荷状況によって、重要度の高い通信は優先して転送できるようにしておくこと

[85] GICTF 副会長の後藤厚宏情報セキュリティ大学院大学教授資料「インタークラウド時代に向けて～GICTF と国際標準化～」より

クラウド単体の構成要素		クラウド間連携に必要な要素	
		ポータビリティ	相互運用性(プロビジョニング含む)
		含めデータ転送できること	
ストレージ		• 異なるクラウド事業者間で、ストレージ内データをスムーズに移行できること	• 連携元クラウドサービスから連携先クラウド事業者へサービス提供に必要なリソースの構成情報とサービスのデータを、自律的に転送できること • 連携元クラウドサービスにて、上記リソースの構成情報とサービスのデータの更新が発生した際は、適宜差分を連携先クラウドサービスへ自律的に転送できること
運用	監視	—	• 連携するお互いのクラウドサービスの各種監視(死活・サービス・リソース・設定)を定期的にできるように、監視プロトコルや各種パラメータを統一しておくこと • クラウドサービス間にてデータ同期が正常に行われているか監視できるようにすること • クラウドサービス間のネットワーク遅延状況を監視できるようにすること
	障害管理	—	• 連携するクラウドサービス間において、クラウド間連携に支障をきたす障害については、適宜情報交換できるようにすること
	構成管理	—	• 連携するクラウドサービス間において、最低限必要な構成情報についてお互い管理できるようにすること • 連携するクラウドサービス間において、時刻同期を実施しておくこと
	切替、切戻し	—	• 切替指示後、速やかに他クラウドサービスへ切替できるように、必要な作業については、ある程度自動化しておくこと • 切戻し指示後、速やかに元のクラウドサービスへ切り戻しできるように、必要な作業については、ある程度自動化しておくこと
	リソース解放	—	• リソースを利用開始した際に起動した仮想マシンやアプリケーションなどの停止やリソース管理情報の更新、移行したデータの完全消去もしくは回収を行えること
セキュリティ	認証	—	• 認証情報のやりとりが可能なこと(シングルサインオン) • 初回認証においては、ワンタイムパスワードや二要素認証などセキュリティ強度の高い認証方式を用いること
	ネットワーク	—	• 利用者～クラウドサービス間通信において、安全にデータ通信が行われること(双方向で安全性確認) • 利用者～クラウドサービス間通信において、不特定多数からのサイバーアタックを防ぐこと • 連携するクラウドサービス間通信において、通信要件のある通信のみ許可すること

出所)GICTF の WhitePaper「インタークラウドのユースケースと機能要件」、インタビュー等より NRI 作成

同図表の各項目について検討された、相互運用性およびポータビリティの確保に必要な主要な技術的要件は以下の通りとなる。

(1) クライアント向け回線(インターネットなど)

災害時、災害復旧時にクライアントから各クラウドサービスにスムーズにアクセスする方式を検討する必要がある。具体的には、DNS バランシングや CDN(Contents Delivery

Network）などを用いて、利用者から異なるクラウドサービスへのアクセスに関して動的に切り替え/切り戻しが可能であることが必要となる。

(2) サーバ（仮想化技術）

ポータビリティの確保については、異なるクラウド事業者の仮想化環境であっても、スムーズに仮想マシンイメージを移行できる環境が望ましい。その場合、標準化され現場での利用が多い OVF の利用が想定される。

また、相互運用性の確保については、災害時は運転要員の操作・処理が的確に行えないことも考えられるので、必要なデータ（仮想マシンイメージ等）が自動的に転送されることが望ましい。また、仮想マシンの構成情報は随時更新されるため、平常時に定期的にバックアップを取得し、連携先クラウドサービスへ同期を行う必要がある。

(3) ネットワーク

クラウド間をつなぐネットワークにおけるポータビリティの確保にあたっては、「IP アドレス」が各ネットワーク部分において重複しないことが望ましい。仮に重複する場合は、クラウド間ネットワークの中間で IP アドレス変換するなど、クラウドサービス間でルーティングを問題なく行い、移行先に問題なく、仮想マシンイメージを含めたデータ転送できることが必要となる。

また、各クラウドサービス内ネットワーク（LAN）とクラウド間をつなぐネットワークにおける相互運用性の確保にあたっては、仮想マシンおよびストレージ内のデータ転送が発生するため、RTO を順守するために遅延を考慮した回線帯域を、クラウドサービス事業の成長に合わせ、双方の事業者で随時検討することが求められる。

また、クラウド間で大容量のデータを送信する場合は、データを圧縮して、回線帯域を抑える方式も考えられる。圧縮にあたっては、専用装置導入等、費用が別途発生するが、回線帯域を抑えることにより、回線費用の削減も見込むことができる。両方を比較し、中長期で考えた時に安価になるのであれば、データ圧縮も検討に入れてもいいのではないかと考える。

(4) ストレージ

ポータビリティの確保については、異なるデータセンター間での転送であっても、スムーズにストレージ内データを移行できる環境が望ましい。

また、相互運用性の確保に当たっては、ストレージ内データが自動的に転送されることが望ましい。さらに、ストレージ内データは適宜更新されるため、平常時に定期的にバックアップを取得し、連携先クラウドサービスへ同期を行う必要がある。

(5) 運用

GICTF の WhitePaper「インタークラウドのユースケースと機能要件」に記載されている 10 の機能のうち、「監視」「切り替え、切り戻し」「リソース解放」の 3 機能に加え、「障害管理」

「構成管理」についても、各々クラウド間連携を実現し運用するための要件が整っている必要がある。

(6) セキュリティ

セキュリティの相互運用性について、「認証」および「ネットワークセキュリティ」の観点から、以下の確保が必要となる。

「認証」について、ユーザの利便性を考えると、異なるクラウド間で ID・パスワード情報を共有し、かつ複数回の認証を避けるため、シングルサインオンの適用が考えられる。その際に、初回の認証対象となるアプリケーションあるいは OS に関するセキュリティ強度が求められる。そのため、ワンタイムパスワードもしくは二要素認証などセキュリティ強度を挙げる方式を合わせて検討する必要がある。

「ネットワークセキュリティ」について、クラウド間をインターネットで繋ぐことを想定した場合、インターネット通信部分の暗号化や、インターネットから各クラウドサービスへのサイバー攻撃への対策が必要となる。

3.1.5. クラウド間連携におけるセキュリティを阻害する可能性のある要素

クラウド間連携におけるセキュリティの阻害要素は、2 種類があると考えられる。

まず、クラウド間連携によって本来はデータセンター内で保護されているデータが外部ネットワークで伝送されることに起因するものである。これは、外部ネットワーク伝送中におけるデータ漏洩、盗聴、毀損が考えられる。これらは、リソース確保、発見時、データ同期のためのデータ転送時、相互サービス監視時、認証連携時の各段階で発生する恐れがある。

もう一つのセキュリティ阻害要素として、保護されているデータを外部ネットワークに伝送する際に、本来保護されている機器（主にストレージ）を外部ネットワークに接続する場合があり、その際にセキュリティ設定の不備により、外部からの攻撃を受ける可能性があるということが考えられる。

3.2. クラウド間連携における契約や取り決め等の要件

3.2.1. クラウド間連携における事業者間の取り決めや契約条件

本章 2 節において各事業者のクラウド間連携に対する認識を把握したが、そこからうかがえる課題をまとめると、「事業者間で異なる契約、サービス価格、サービス仕様（セキュリティポリシー含む）、クラウド構成（データモデル、各種 API 等）の差異をどう解決するか」である。裏返すと、課題と思われる差異の部分について、予め事業者間で取り決めをしておくことで、異なるクラウド事業者間連携がスムーズに行われるのではないかと考えられる。契約、サービス価格、サービス仕様について、何かガイドライン的なものがあるわけではなく、それよりも競争原理による差別化志向が出てくるため、当然内容は違うものになる。また、

構成面において、前に述べた各クラウド標準化団体が策定した共通仕様を各クラウド事業者が採用していれば問題ないが、実際には事業者に受け入れられているものと、そうでないものと、まだ混然としている状態であり、構成面においても事業者間の取り決めが必要となってくる。

一方、事業者からのインタビューでは出てこなかったが、事業者間連携を具体的に考えた時に、災害時の切り替えトリガをどうするかという取り決めが必要と考えられる。重要システムである場合は、事業者ではなく、行政による切り替えの発動も検討する必要がある。

以上の理由から、クラウド間連携を行う際に事業者間で取り決める必要のある内容は以下のようにまとめられる。それぞれ事業者間で前もって確認しておくことが重要である。

図表 106 クラウド間連携における事業者間の取り決めとその内容例

項目	内容
クラウド間連携の発動	・ どのような場合に連携先に切り替えるかを定めておく必要がある。 ・ 重要インフラの管理システムの場合は、事業者間で定めるだけではなく、行政によって発動タイミングが決定される可能性がある。
SLA およびサービス仕様	・ 連携するクラウドサービス間の SLA およびサービス仕様（外部向け、内部向けともに）の差異がわかるように、お互いに開示するとともに、差異がわかるように標準的な様式を利用して示す必要がある。 ・ SLA およびサービス仕様取り決め後に変更があった場合は、変更したことが速やかに連携先にわかるようにする必要がある。
セキュリティポリシー	・ 連携元と連携先のセキュリティポリシーを完全に一致させるか、最低ラインのみを適合させるか定める。 ・ 連携のためにセキュリティポリシーを開示することにより、連携先クラウド事業者からのセキュリティアタックが発生した場合に備えて、別途契約を取り交わしておく。
ビジネスモデル	・ 連携を行った場合の費用と収益の配分ルールを前もって定めておく必要がある。
データモデル	・ 連携するデータ構造やデータの配置場所等（ローカルディスク、NAS など）を取り決める必要がある
各種 API	・ クラウドサービス切り替え時に必要なアクション（VM 起動やデータ転送等）を自動化するために、各サービスで設定されている API 情報を相互に公開する必要がある。

3.2.2. データセンター間連携やクラウド間マイグレーション実施時に、クラウドサービスの利用契約が事業者間で移転することもしくは再委託の構造が発生することに関する利用契約上の条件や規定事項

前項の取り決めを事業者間で確認するのみならず、クラウド間連携を行う予定のあるシステムのユーザに対しても告知する必要がある。そのために、利用契約や約款等をデータセンター間連携やクラウド間マイグレーションを行う前提で取り交わす必要がある。

ユーザに提示する必要があると思われる項目は以下のものである。

・ クラウド間連携を実施することに関する基本的な合意の規定

・ 実施の条件（どのような条件で実施するのか）
　（例） 法令で定める「激甚」に相当する大規模災害の発生した場合
　　安定的な電力供給が確保できない場合　 等
・ 連携先（再委託先）の条件
　（例） 契約時に指定した事業者に限定する。
　　有事において、クラウド事業者と利用者の合意に基づき決定する。
・ 連携時におけるサービス水準
・ 個人情報、知的財産等の機密情報の取扱いに関する規定
・ 料金に関する規程（サービスの範囲内か、追加料金が発生するのか、その場合どのような料金体系となるのか）

なお、もとの利用契約がライセンス契約、業務請負契約、準委任契約、といった契約形態のどれに該当するかによって、条件や規程事項は変わりうることに留意が必要である。すなわち、ライセンス契約や業務請負契約の場合、事前にすべて規定しておく必要がある一方、準委任契約の場合は、状況に応じた対応が可能で、柔軟に運用することが可能とされている。

図表 107 契約形態別の留意事項

	請負契約	準委任契約
特徴 （関連法規）	根拠法：民法 委託先の特定個人ではなく組織としての総合力を期待しての契約。	根拠法：民法 完成責任はないが、進捗報告義務、終了報告義務、善管義務がある。
業務内容	受託者が一定の業務を完成してその結果に対して発注者が報酬を支払う。完成の判断は、成果物の検査合格または報告書の確認。	発注者が一定の業務処理を一任し、受託者がそれを承諾し、善管義務をもって業務を処理する。
瑕疵担保責任	受託者は期限内で補修や損害賠償などの担保責任を負う。ただし契約により変更可能である。	善良なる管理注意義務をもって遂行すればよく、瑕疵担保責任はない。

出所）長尾清一「先制型プロジェクト・マネジメント」ダイアモンド社より、NRI 作成

3.2.3. データセンター間連携やクラウド間マイグレーションの際に障害となりうる民法その他の法令上の制約と、その回避のために整えられるべき条件

データセンター間連携やクラウド間マイグレーションの際に法制度上障害となり得るのは民法では「瑕疵担保責任」と「緊急避難」の条項であると考えられる。業務請負契約の場合、クラウド間連携を実施したが、期待したレベルのサービスを提供できなかった場合、どこまで瑕疵担保責任が問われるかが不明確になる恐れがある。このため、事前にサービスレベル契約等で、明示的に条件設定をしてリスクを回避することが必要であると考えられる。

また、有事の際にクラウド間連携を行うことが、緊急避難に該当するかどうかは、事案ご

とに状況が異なるため、一律に該当・被害等を決定することができない。その結果判断基準や結果責任が曖昧になる可能性がある。そのため、契約でクラウド間連携をする場合の条件を明示することで、曖昧さを回避することが求められる。

民法以外の法令においては、個人情報保護法、著作権法、不正競争防止法、消費者契約法がデータセンター間連携やクラウド間マイグレーションの際の制約条件となる可能性がある。以下その可能性の概要について記す。[86]

個人情報保護法

個人情報保護法においては、第三者提供の禁止規定が存在するため、個人データを含んだ情報を事後的に第三者の管理下に置くことが困難と考えられる。そのため、事前に、クラウド間連携を行うことを、ユーザ企業だけでなく、エンドユーザにも利用契約の中で包括的に同意を取得しておく必要があるものと考えられる。

著作権法

著作権法では、著作権者に「複製」と「公衆送信」を行う権利を与えているため、著作権者の許諾無くコンテンツを複製したり、インターネットを通じて不特定多数の者に当該コンテンツを配信したりする行為は禁じられている。クラウドに格納するデータが著作物性を持つかどうか事前に確認が必要である。

不正競争防止法

不正競争防止法では、秘密として管理され、非公知、かつ有用な情報を「営業秘密」と定義し、同情報を不正に取り扱う行為を不正競争としている。クラウド間連携等の際にはセキュリティを確保して、同法に抵触しないよう留意が求められる。

消費者契約法

消費者契約法では、消費者との契約において、事業者の損害賠償の責任を免除する条項の無効が規定されている。すなわち消費者保護の観点から、利用規約で免責事項を定めていても、同法によって無効とされることがありうるということである。Web メールのように、消費者に直接提供しているクラウドサービスに適用されることが想定される。

3.2.4. 異なる司法管轄にあるデータセンターまたは事業者間で行われるときに、移行・移転の前と同等の、利用者にとっての法令上の権利義務等が確保されるために必要な国際連携に関する要件

86 岡村久道「クラウドコンピューティングの法律」民事法研究会（2012 年 2 月）を参考に作成

データセンターの位置によって一義的に準拠法が定まることは通常ないと考えられるので、国際司法・国際裁判管轄の規程については、契約によって明示することが必要である。このことにより、準拠法の指定を明確にして移行・移転前と同等の権利義務等を確保することが求められる。

しかしながら、準拠法、管轄裁判所の指定を契約書上で合意しても、データセンターが外国に所在する場合、同所在国の警察等の執行機関による捜索・差し押さえリスクは残る。そのため、捜索・差し押さえリスクを受容できる国に所在するデータセンターへ移行・移転することが望ましい。

クラウドにおいては、データの所有権、データの管理責任、サービスの提供・利用契約、設備の貸与・利用契約等、権利や契約の関係が複雑になる。これらが複数の司法管轄にまたがって締結され、存在する状態も容易に想定される。クラウドの円滑な利用、緊急時の柔軟なマイグレーションや総合運用を考えた場合、国際的に一律な法的解釈や取り扱いがなされれば、事業者もユーザもその提供・利用をより積極化でき、クラウドの信頼性を高めるのに資することになる。このような国際的取り決めの実現に向けた取り組みが提起され、推進されることが期待されるところである。

IV. 今後官民が取り組むべき課題の提起

1. クラウド事業者およびその他の事業者、社会システムが満たすべき要件の全体像

今まで見てきたように、クラウドは人々のコミュニケーションや企業活動の基盤、あるいは社会の重要なインフラストラクチャーを管理・運営する情報システムの基盤として多くの場面で使われるようになった。また、先の東日本大震災においても被災したシステムの代替サービスや刻々と変化するニーズに対応した情報サービスの提供を迅速に行うことができ、クラウドの持つ特性が緊急時において有効であることが明らかとなった。

さらに、今回の災害においては、一部で小規模な被害はあったものの、主要なクラウドデータセンターではサービスの継続ができたことで、大規模災害におけるクラウドの可用性の高さが改めて示されている。

しかしながら、併せて課題も明らかとなった。クラウドのデータセンターそのものは被害が少なかったものの、長時間の停電や計画停電の実施で自家発電燃料の確保が難しくなるケースも見られた。また、ユーザ環境やユーザからのアクセス回線が被災または停電したりすることによって、データセンターは稼働しているもののサービスが利用できないケースがあった。

以上のことから、分散的に処理されるために本来は災害等のインシデントに強いクラウドの可用性を高めるために次のことが必要になるものと考えられる。

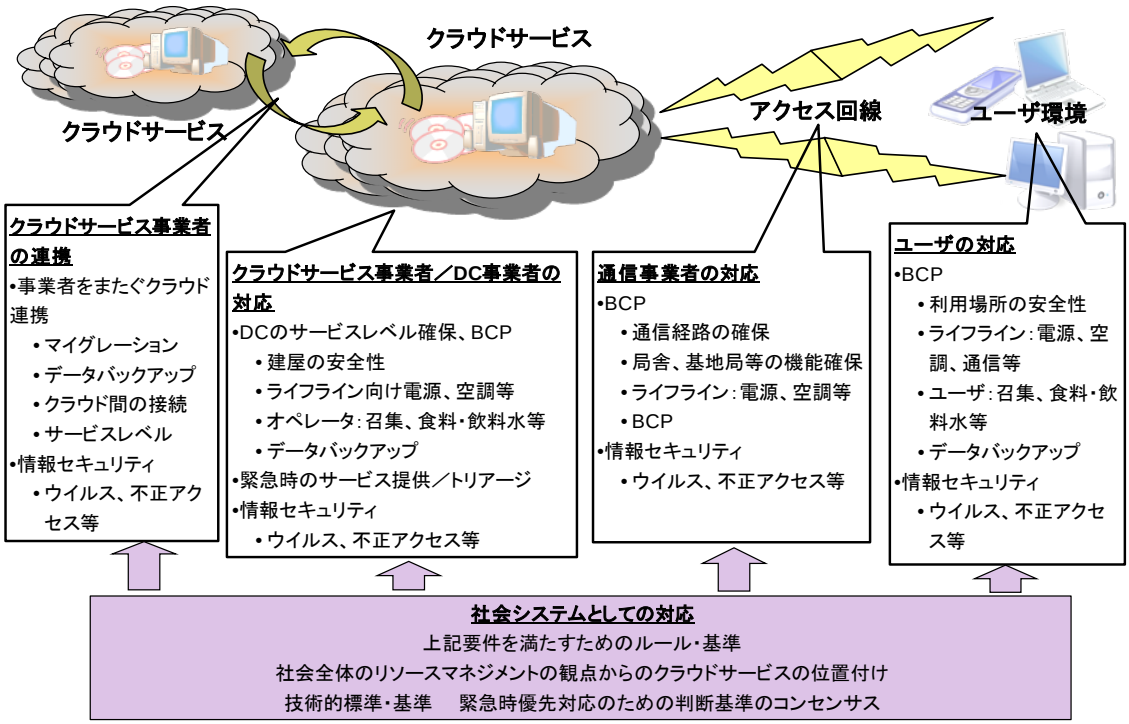
まずクラウド事業者・データセンター事業者の対応としては、クラウドのサービス維持能力の強化を図ることが望まれる。具体的にはデータセンターの BCP、ライフラインの強化等を行うことである。次に、通信事業者の対応としては、データセンターとユーザ間の通信回線の可用性の確保であり、そのための通信網の耐災性の強化が求められる。さらにユーザの取り組みとして求められるのは、利用場所の安全性の確保やデータバックアップ等である。

また、これらの施策を講じたとしても、クラウドサービスそのものが利用できなくなる事態も想定される。その場合にはクラウドをまたがったシステムやデータのバックアップ、さらには他のクラウドでのシステム稼働なども想定しなければならない。

しかし、これらを進めていく上では、社会全体としてクラウドサービスが重要な位置を占めていることを認知した上で、災害や異常事態に対する対応の中で一定程度の優先度をもって対応することへのコンセンサスを得る必要があるものと考えられる。

これらのことを図示すると図表 107 のように示される。

図表 108 クラウドのサービス継続・障害対応を強化するための全体像



2. 官民が取り組むべき課題

2.1. 基本的な考え方

事業者、利用者等の個別の取り組みを促進するために、社会全体として取り組まねばならないことは以下の 3 つであると考えられる。

2.1.1. クラウドの社会インフラとしての明確化

クラウドが社会に徐々に浸透していることは実態調査で明らかになった。しかしながら、クラウドはユーザからは見えにくい。そのため、社会全体から見たときに、クラウドが担っている役割が過小評価される可能性がある。現状においても、事業継続性の確保が事業者やユーザなどの民間企業の努力のみに委ねられている状態にあると見られる。

そのため、クラウドが国民生活を支えており、社会システムや重要インフラの運用を担っている、社会のインフラであるとの位置づけを明確化することがまず重要であると考えられる。

たとえば、重要インフラを支えるクラウドや国民の生活やコミュニケーションに不可欠なクラウドなどについては、電力、上下水道や電話ネットワークと同様に、防災計画など、緊急

事態に備えた計画に盛り込み、そのサービス確保を社会全体として行うべき課題と位置づけていくことなどの方策が考えられる。

また、今後参入事業者が増加するにつれて高まるサービス停止リスクに備え、現行の情報開示制度をさらに充実させるとともに、保険や供託金、代替サービス紹介などの社会的なセイフティネットの整備も望まれる。

2.1.2. 多様な災害・障害に対応するためのサービスの優先順位付け

今回の東日本大震災でも、事前の被災想定を越える規模の災害が発生した。今回は、クラウドを支えるデータセンターに大きな被害はなかったものの、地震だけではなく、水害、火災、サイバー攻撃等の多様な災害・障害要因が発生しうる。また、その大きさも発生地点も様々であると考えられる。

これらすべてのリスクについて、あらかじめ対応計画を立案することは非現実的である。そこで、前もってどのサービスをどの程度まもる必要があるか、守るべきかについて優先順位とサービスを確保する範囲を定め、それについて社会的な合意を得ておくことが望まれる。

具体的には、社会インフラ、企業の業務インフラ、国民のコミュニケーション等を支えるクラウドそれぞれについて、最低限維持すべきサービスレベルを規定するとともに、必要最小限までに縮退させる順位付けとそれぞれのサービスにおける BCP の強化を図ることが望ましい。

2.1.3. クラウド間連携に向けた社会制度の確立

クラウド間連携は、まだ国内でも先進的な取り組みが始まったところであるが、BCP や災害対応を考えたときに有力な手段であると考えられる。また、オンプレミスのシステムのバックアップとしてクラウド連携を用いる考え方も徐々に出てきている。

欧米ではビジネス上の制約から、クラウド間連携の取り組みが進んでいない中、日本の被災経験などを活かして、国際的な取り組みに貢献し、たとえば標準化活動を牽引していくことには大いに意義があると考えられる。

また、クラウド間連携の技術的な側面のみならず、事業者間の契約、取り決めやユーザと事業者間の契約、さらには現状で障壁になる恐れのある個人情報保護法、著作権法、不正競争防止法、消費者契約法等の見直しを行って、クラウド間連携を前提とした制度設計を進めていくべきである。

図表 109 クラウドのサービス継続性確保に向けて官民が取り組むべき課題

	課題	取り組みの方向性
社会インフラとしての位置づけの明確化	・ 行政の防災担当者がクラウドコンピューティングが重要インフラを担っていることをあまり認知していない ・ 事業継続性が民間企業の努力にのみ委ねられている	・ 重要インフラを担うクラウドの「防災計画」等への組み込み ・ 社会インフラとして重要度を増すクラウドの一部を重要インフラと位置付けて、然るべき対応を組み込むこと

多様な災害・障害に対応するためのサービスの優先順位づけ	・ あらゆるリスクに対応して前もって対策を立案することは不可能 ・「想定外」の事態に備える必要がある	・ クラウドサービス全体としての BCP の確立 ・ 災害・障害発生等緊急時の対応に関する優先順位付けの考え方の確立と社会のコンセンサス獲得(トリアージ)
クラウド間連携に向けた社会制度の確立	・ クラウド間連携については日本以外での検討は進んでいない	・ 国際規格策定に向けた日本のリーダシップの発揮 ・ SLA、契約、個人情報保護制度などを、クラウド間連携を前提として見直し

2.2. 具体的な施策

最後に、クラウドサービス継続やデータセンター間連携、クラウド間マイグレーションの実現のためにそれぞれの主体が行っていくべきことをまとめる。

2.2.1. サービス継続のための施策

サービス継続のためには、クラウド事業者は自らの BCP の強化を行っていくとともに、通信事業者等の関連事業者と協力して、エンドユーザ環境まで視野に入れたサービス継続手段の検討を進めるべきである。特に、中小企業等で IT 管理力の高くないユーザに対しては、サービスベンダーとして積極的に提案していくことが望ましい。このことは提供するサービスの価値を高めることにもつながるが、ユーザ側のコスト低減ニーズとのバランスを考える必要がある。

ライフライン事業者等の関連事業者についても、自らの BCP を強化するとともに、二次サプライのサプライヤを中心に、特に重要インフラを担うクラウドに対して、優先的にライフラインの確保を行うことを検討すべきである。優先順位づけに当たっては、関係ステークホルダーの合意形成が必要となるため、行政からもサポートが提供される中で進めていくことが望まれる。

ユーザ企業においてもクラウド事業者と協力の上、BCP を強化すべきである。

一方、社会全体については前述したように、クラウドを防災やリスク対応の枠組みに位置づけ、たとえば行政が策定する防災計画の中でサービス確保のための支援方策について検討していくべきであると考えられる。また、セイフティネットの整備にあたっても行政に期待される役割は大きいものと考えられる。

2.2.2. データセンター間連携、クラウド間マイグレーション実現のための施策

クラウド事業者自ら、または業界団体が標準規格を整備したり、データセンター間連携、クラウド間マイグレーション(移転)に当たっての SLA、契約ならびに規約等の整備を進めていくことが望ましい。また、技術的な適用可能性を検証するため、技術実証を行って実運用の早期の実現を目指すことが期待される。

また、行政は業界が行う上記の取り組みを支援するとともに、実現の阻害要因となり得る

個人情報保護等の法制度について、クラウドならびにその連携を前提としたものに見直しを行ったり、商習慣等を同様に変革していくに際しての先導的な役割を担ったりすることが望まれる。

図表 110 サービス継続、クラウド間連携のための具体的な施策

	サービス継続	データセンター間連携 クラウド間マイグレーション（移転）
クラウド事業者	• BCP の強化 • エンドユーザ環境まで視野に入れたサービス継続の検討 • 情報開示の強化	• 標準規格の制定・採用 • SLA／契約／規約の整備 • 技術検証と実運用の実現
関連事業者 （ライフライン等）	• BCP の強化 • 重要インフラを担うクラウドに対する優先度の向上	－
通信事業者	• BCP の強化 • クラウド向け通信サービスの優先提供	• クラウド間マイグレーション（移転）のための通信路の確保・優先提供
ユーザ	• BCP の強化	－
行政 社会全体	• 防災、リスク対応の枠組みへのクラウドの位置づけ • 情報開示、セイフティネット構築等の業界の取り組みの支援	• 技術規格化、標準化等の業界の取り組みの支援 • 個人情報保護等の第三者提供禁止規定などの法制度について、クラウド間連携を可能にすることを視野に入れて見直す

おわりに

以上見てきたように、クラウドコンピューティングは社会に浸透しつつあり、今後電力や電話、水道、交通のような社会基盤サービスとして位置づけられていくものと予測される。また、分散処理、仮想化という特性を活かして大規模災害時の対応でも威力を発揮することが明らかとなった。

しかしながら、クラウドコンピューティングは発展途上の技術であり、技術開発の面およびそれをサービスとして社会に適用していく面の双方において、解決すべき課題が存在することも明らかとなっている。たとえば、災害時におけるクラウドサービスの運用継続性においては電源を中心としたライフラインやその代替サプライにおいて課題を残しているし、クラウド事業者をまたがったシステムやデータの連携、マイグレーションについても検討の途上である。特にデータセンター間連携やクラウド間マイグレーションについては我が国での検討が先行していると考えられ、国際的な貢献も期待される。

また、社会的な合意形成や制度構築も求められる。災害や障害時におけるリソース制約下では、ある程度の縮退運用を行う必要がある。個別のサービスでの事前の条件設定はもちろん必要だが、大規模災害等では複数のユーザ、サービスのうちどれを優先的にサービス継続させるかについて、社会的な合意形成が必要である。これにあたっては行政が主導となって優先順位を検討していくことが望まれる。

さらに、中小事業者等を含めた品質保証、品質管理の在り方についても社会システムの整備が求められる。ユーザが安心してサービスを選択するための事前情報開示はもちろん、品質を保証するための認証等の制度の創設や、サービス停止や事業者の破綻などの際のセイフティネット構築等、業界や行政等が連携して検討を進めていくことが求められる。

このように、技術面、社会制度面の両面からクラウドを安心、安全に利用できる環境を整備していくことで、クラウドが社会に普及するとともに、IT による効率化や付加価値の向上等の恩恵を広く享受できるようになると期待される。クラウドは、社会インフラを担い、緊急時には平時の機能を維持・回復するだけでなく、緊急時に新たに発生するニーズへの対応が期待できる。これは、クラウドの耐災性、拡張性、迅速性などの特性によって可能になる社会的機能と言える。

同時に、社会を支えるインフラの一環を担うクラウドコンピューティングの、万一の事故や停止が社会に及ぼす影響はそれだけ大きくなる。それを最小限にできるような技術や仕組みの構築、進化が進むことを期待したい。

本報告書がその検討の端緒となり、条件・環境整備の一助となれば幸いである。

以上