ＢＣＰの対策として

クラウドをどう活用できるのか

一般社団法人 日本コンピュータシステム販売店協会
サポートサービス委員会

© 一般社団法人 日本コンピュータシステム販売店協会 2012

はじめに

東日本大震災から早くも1年が経過しようとしています。復興はまだ緒についたばかりで、これからもまだまだ、幾多の困難があると思われます。販売店協会も引き続き協力をしていく所存です。

協会の委員会の1つとして、サポートサービス委員会は一昨年、【やさしい「ITサービス継続」】と題した解説書の中で、ITサービス継続とは？から始まり、災害への対策・運用面の対策・各種フェーズでの対策などを、分かり易く説明しました。（詳細は平成23年度の報告書をご参照ください。）各企業では、大震災発生時にも事業を続けるための施策として、BCPが策定されていますが、昨年度の大震災でそれらは有効だったのでしょうか。本解説書では、BCPの1つの施策としてのクラウドとの関係についてご理解頂くことを目的としています。

大きな震災発生時でも、事業の中断を避けるためにどんな対策をとっておけば良いのか。その1つの選択肢としてのクラウドを有効に利用できるようにするにはどうすれば良いのか、本解説書からヒントを得て頂ければ幸いです。

一般社団法人　日本コンピュータシステム販売店協会
サポートサービス委員会

目次

© 一般社団法人 日本コンピュータシステム販売店協会 2012

1. BCPについて

1.1 BCPとは

BCPとは事業継続計画（Business Continuity Plan）のことで、自然災害や事故、感染症、テロなどの緊急事態が発生した場合に企業の重要業務を停止しないよう策定する計画のことです。

万が一業務が停止しても被害を最小限に抑え、目標復旧時間内に重要業務を再開させるための手段を取り決めておくこともBCPの重要な役割です。

例えば、長時間の停電に備え非常用発電機を準備することや、工場や事務所を2カ所以上保有し、業務停止が発生した際には影響の少ない工場、事務所にて業務を引継ぎ再開できるような準備を進めておくなどの二重化を採用することによりリスクを分散することができるのもその一例です。

最近ではBCPを策定する企業も増えてきてはいますが、策定するのみで終わってしまうことも多いようです。いざという時に有効に機能させるためにも、平常時からテストや訓練を実施し、問題点があれば改善し、繰り返し見直していく取り組みがとても重要です。

1.2 BCPの必要性

なぜBCPが必要なのでしょうか？自然災害やテロなど、予期せぬ事態が発生した場合、その影響により倒産や事業縮小を余儀なくされるケースが少なくありません。このような緊急時に事業資産の損害を最小限にとどめ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段などを事前に取り決めておく必要があります。

1.2.1 BCP策定の考え方

BCP策定を進めるにあたって下記の様な手順を踏みます。

①リスクと業務への影響を洗い出す
②ビジネスを継続するために優先的に復旧すべき業務とそれに必要な設備やシステムを明らかにする
③目標復旧時間や復旧手順を決める

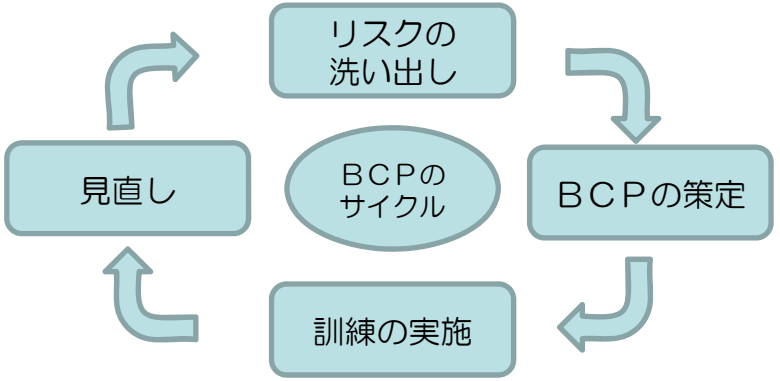
例えば、①のリスクとして大規模な地震を想定すると建物の崩壊や停電、断水などが考えられます。仮に建物が無事でも、長期間停電が続けば、その間は情報システムや工場の機器が動かないため、業務は止まったままになります。

②は、会社の生命線となる業務を優先して、復旧の準備体制を作ります。例えば、商品の生産が会社の生命線とすれば工場の再開が第一となり、そのために生産管理システムが必要なら、サーバルームの耐震化、自家発電装置、バックアップシステムなどを整えます。

これを受け③では、どのタイミングで自家発電装置を動かしたり、バックアップシステムに切り替えたりするのか、また、誰がそれを指示するのか、といった復旧手順を定めます。

実際の災害時には、社員の安全確認など人的な面も重要です。業務の比重の変化も含めて全社的な見地から、定期的にBCPの見直しと、模擬訓練を実施する必要があります。

参考：日経コンピュータ「情報システムハンドブック」
（C）日経BP社　2010.1.1更新



1.2.2 企業を取り巻くリスク

企業を取り巻くリスクは多様であり、事業への影響の内容や規模もリスクによって異なります。各リスクの事業に対する影響や地域の災害特性、各企業の特徴などを考慮して、リスクへの対策を実施することが重要です。

以下は、中小企業庁の「中小企業BCP策定運用指針」を参考に作成しています。

(1) 地震

発生頻度は他のリスクと比較して相対的に低いものの、突発的な災害であるため、施設などの物的被害だけでなく、従業員や顧客などに死傷者が発生する可能性があります。また、交通やライフラインといった社会インフラ機能への影響も大きく、事業の回復にも時間がかかります。このため、耐震化などの予防対策や避難や安否確認などの応急対策に関する検討が求められます。

(2) 風水害

地震と異なり警戒が可能であるため、適切な対応を実施すれば被害の予防・低減が可能であり、従業員や顧客などの死傷者が発生する可能性は低くなります。

また、交通やライフラインといった社会インフラ機能が致命的なダメージを受けにくく回復も早いため、事業の回復も、地震より一般的に早くなります。

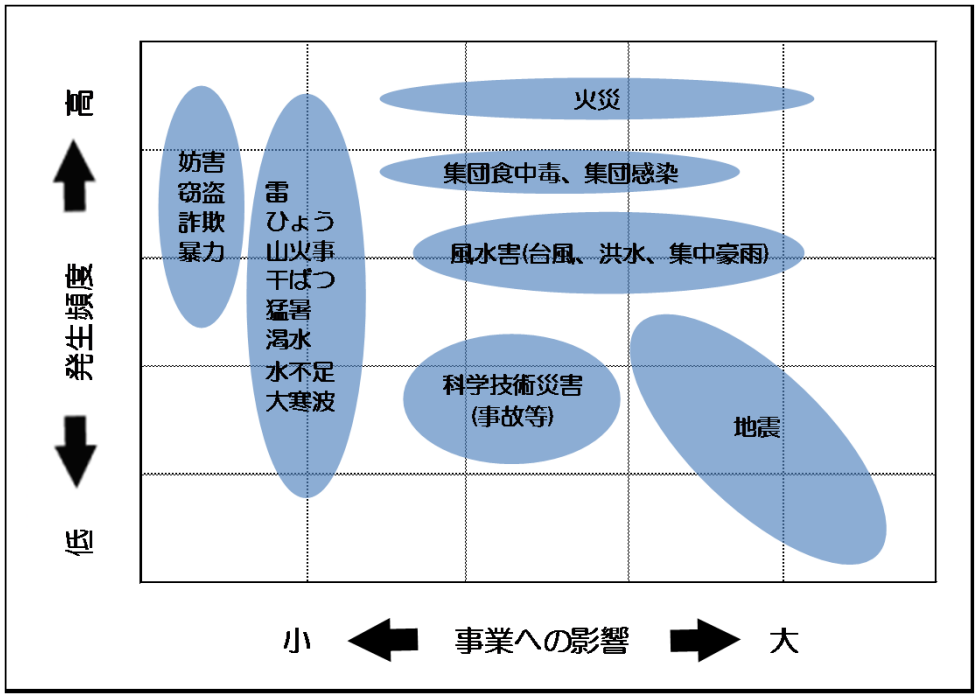


図　企業を取り巻くリスク（イメージ）

出典：中小企業庁「中小企業BCP策定運用指針」

⑶ 火災

広域的な被害は無いものの、当該企業には死傷者の発生や施設の全焼など、致命的なダメージを与える可能性があります。また、隣接する企業や住宅に延焼する可能性もあります。

⑷ 従業員の集団感染・集団食中毒

従業員の集団感染・集団食中毒では、原因となるウイルスなどの種類にもよりますが、最悪の場合には死者が発生する可能性があり、また死者が発生しない場合でも多くの従業員が一定期間就業できなくなるため、企業活動の停止や低下を伴う可能性があります。また、商品などを経由した外部への2次感染の可能性も考慮する必要があります。集団食中毒については、イベントなどで全従業員が同じ弁当を食べないといった予防対策が求められます。

⑸ 科学技術災害

危険物の施設・輸送事故、電力供給停止などが含まれます。化学メーカーなどの場合には当該企業の事故などが原因となる場合もあり、直接的な被害と共に事故を起こした社会的責任から事業再開が困難になるなどの重大なダメージを伴う可能性があります。

⑹ その他の自然災害リスク（雷、ひょう、など）

雷やひょう、猛暑、渇水・水不足などの、地震や風水害以外の自然災害が含まれます。相対的に発生頻度は高いものの、人的被害や物的被害を伴う可能性が非常に低いため企業活動に重大な影響を与える可能性は低くなります。しかし、商品の売上げが気候に左右されやすい場合や、水不足や大寒波などの影響を受けやすい企業では、深刻な問題となる場合もありますので、当該企業はこれらのリスクへの対策が必須となります。

⑺ その他の人為的リスク（企業内暴力、妨害、窃盗、コンピュータ犯罪など）

企業内部の暴力や外部からの妨害や窃盗、コンピュータ犯罪などが含まれます。これらに遭遇する可能性は、他のリスクより相対的に高いと考えられますが、被害対象が限定されるため企業活動に重大な影響を与える可能性は非常に低くなります。ただし、コンピュータ犯罪では、発注や生産管理などの基幹システムに支障が生じた場合、企業活動に一定期間支障が生じることも考えられます。

1.2.3 BCPの重要性

緊急時対応シナリオ（中小企業庁「中小企業BCP策定運用指針*」）を通して、BCPが策定されている場合とそうでない場合を比較し、被害・復旧の違いを見てみましょう。

次頁の表は、数例あるシナリオから製造業の地震被害の場合を抜粋したものですが、BCPを導入している場合とそうでない場合の、復旧状況とその影響度合が良く分ります。

これは一例ですが、BCPの策定と訓練、見直しの繰り返しが、緊急時の事業継続への影響度、復旧速度を左右する重要なカギとなります。

---

*:下記URL参照
http://www.chusho.meti.go.jp/bcp/contents/level_c/bcpgl_08_04_1.html

事例：製造業（地震災害）

	BCP導入なし企業	BCP導入済み企業
想定	・自動車用部品などのプレスメーカ（従業員３０名）。 ・平日早朝、大規模地震が突発発生、県内の広い範囲で震度6強を観測。	
当日	・工場では、すべてのプレス機が転倒。 ・ほとんどの従業員の安否確認ができず。 ・納品先に連絡するが電話が通じず、その後、後片付けに追われ納品先に連絡せず。	・工場ではアンカーを打っていたためプレス機の転倒は免れる。 ・伝言ダイヤル171で大半の従業員の安否確認ができる、伝言のない者については近所に住む従業員に自宅まで様子を見に行かせる。 ・納品先に連絡するが電話が通じないため、最寄りの営業所まで従業員1人をバイクで事情説明に行かせる。
数日間	・従業員は家族の被災や地域活動のため半数が1カ月間出社せず。 ・原材料の仕入元会社の工場が全壊、代替調達の目処が立たず。 ・１週間後、納品先の大企業から発注を他会社に切り替えたとの連絡あり。	・従業員に対して日頃、耐震診断済みのアパートに住むよう指導していたので家族の被災を免れる。 ・大半の従業員が、3日間は地域活動に専念、その後1カ月間は2/3が出社するよう交代制をとる。 ・中核事業である自動車用部品の生産復旧に最優先で取り組む。 ・原材料の仕入元会社の工場が全壊するが、あらかじめ話をつけていた会社から当面の代替調達を行う。 ・プレス機械調整のため、協定どおりメーカーから技術者受け入れ。 ・3日後、納品先の大企業に、目論見通り1カ月で全面復旧可能と報告。 ・この間、納品先の要請で、他会社（金型が互換できるようプレス機の種類をあらかじめ統一）での代替生産のために従業員を派遣。
数カ月間	・3カ月後、生産設備は復旧するも、受注は戻らず。 ・プレス機械の更新のため金融機関から融資を受ける。 ・会社の規模を縮小、従業員の７割を解雇。	・手持ち資金により、従業員の月給、仕入品の支払を行う。 ・同業組合から、復旧要員の応援を得る。 ・１カ月後、全面復旧し、受注も元に戻る。 ・損壊した一部プレス機械の更新は地震保険でカバー。 ・震災後、納品先の信用を得て、受注が拡大。

出典：中小企業庁「中小企業BCP策定運用指針」

1.3 トラブル事例

1.3.1 東日本大震災のシステム被害状況

（記事：日経コンピューター　2011.03.31号を基に最新情報追記）

＜青森県＞

・H市役所

　システムは破損せず。停電時は、UPSや自家発電装置を使って住民票発行などの住民サービスを継続。プロバイダーのシステムが停止したので電子メール、ホームページは使用不可に。いずれも3月12日夜に電力が戻り復旧。

・大手金属鉱業　M社

　八戸市にあるグループ企業の製錬工場が津波で浸水。海水に漬かったため通電できない状態が続く。6月10日より操業。受注や購買、在庫管理などのシステムは、本社で集中管理しており被害なし。

・地元ショッピングセンターチェーン　U社

　47店舗のうち一部が被災し、建物や店舗系システムが被害をうけた。

＜岩手県＞

・O町役場

　住民基本台帳サーバをはじめとしたハードが破損し1カ月にわたり行政機能が停止した。後に災害に

強い行政を目指し、行政に関する情報をデータセンタに保存する「自治体クラウド」の導入を決めた。

・T市役所

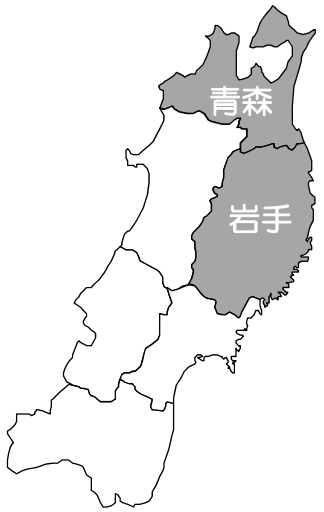
　市庁舎が崩れ、一部の端末が破損したがサーバは無事。停電でシステムがダウンしたが3月13日夜に電力が戻り復旧した。

・大手電気機器メーカー　T社

　北上市の半導体製造子会社が被災。生産システムよりもむしろ生産設備の被害が大きく、3月28日から一部ライン立上げ、4月11日から一部生産再開。

・地元ショッピングセンターチェーン　J社

　POSレジなど店舗系システムが被害を受けた。3月15日の電力復旧以降、徐々に業務を再開。



＜宮城県＞

・M町役場
　役場の建物が全壊し、住民関連データを格納したサーバが流されたが、戸籍データ副本が発見され、最悪の事態は免れた。

・S市役所
　市内にある情報システムセンタ内のサーバは損害がなかったが、区役所や出先機関と接続するネットワークに障害が発生。

・大手電気機器メーカー　S社
　多賀市の磁気テープやブルーレイディスクの生産工場が被災。津波により、がれきが工場構内に流れ込んでおり浸水被害。

・地元ショッピングセンターチェーン　A社
　本部系システムの被災は少ないが、VANとの通信に被害があり、発注業務に支障。店舗系システムにも被害。4月30日に、津波にて全壊した1店舗を除き30店舗にて営業を再開。

＜福島県＞

・県庁
　庁舎の電源が壊れ、サーバが動作せず、住民票の発行などほとんどのサービスが一時提供不能に。

・大手ショッピングセンター　B社
　本部系システム、店舗系システムともにほぼ問題なし。3月12日には170店舗中105店舗が休業していたが、電力の復旧に合わせて順次営業再開し、4月1日には10店舗を除き営業再開。10月現在では津波・原発の影響を受けた7店舗が休業中。

＜茨城県＞

・県庁
　地震直後は停電になったが、非常用電源が動きシステムは停止せず。

・大手電気機器メーカー　H社
　県外含め、7つの生産拠点にて建物と生産設備の被害を受けた。

＜その他＞

・大手銀行　Y社
　停電の影響で3,000台のATMが一時利用不能となる。

・大手スーパーマーケットチェーン　I社
　本部系システムは被災していない地域のデータセンタで集中運用していたため、問題はなし。東北地域の全170店の9割以上は営業再開。

・大手スーパーマーケットチェーン　Y社
　システムは基本的には問題なし。東北地域の全10店は営業再開。

・大手コンビニエンスストアチェーン
　システムの詳細な稼働状況を把握できていない店舗もあるが、システムの故障よりも停電と通信トラブルの影響が大きい。店舗は順次営業を再開。

1.3.2 災害対策事例から見るBCPのポイント

中小企業庁ホームページ内にある、資料『中小企業の事業継続計画（BCP）＜災害対応事例から見るポイント＞』*は、新潟県中越地震、能登半島地震、新潟県中越沖地震で被災した中小企業経営者に、「被災時の状況」とそれによる「事業継続の危機にどう対処し」、「どのように事業を継続することができたのか」という点についてヒアリングした事例です。また、BCP対策をする上で考慮すべき点が下記の項目にまとめられています。非常に参考になりますのでご紹介します。

①従業員の安否確認
②復旧目標の表明とリーダーシップ
③継続する業務の選択
④代替手段の有効性
⑤分散化の効果
⑥復旧資金の確保
⑦取引企業からの支援
⑧従業員の勤務体制
⑨情報発信の効果
⑩耐震措置や訓練の効果

---

*:下記URL参照
http://www.chusho.meti.go.jp/keiei/antei/download/110531Bcp-Reserch.pdf

事業継続計画（BCP）の項目／例

	項 目	内 容
1.前提	**想定する事態**	どのような事態(事業リスク)に対応するための計画なのか、前提を明確にする。 ＜ここでは大規模地震を想定＞
2.事前の対策	**① 耐震措置などの実施**	建物や設備の耐震措置や防災設備の導入などの耐震対策を講じる。
	② 代替方法の確保	事業継続に不可欠な設備・施設などが使用不能になった場合の代替方法を検討し準備しておく。
	③ 分散化の実施	在庫の保管、設備・施設の設置、取引先の所在地域などについて地域的な分散化を図る。
	④ 優先業務の特定	最優先で復旧・継続すべき業務は何か、あらかじめ検討しておく。
	⑤ 地震保険などの活用	保険や共済などの制度について内容を検討し活用する。
	⑥ 安否確認の方法	経営者及び従業員の安否確認の方法を定め、定期的に訓練を行う。
	⑦ その他	（各社の必要に応じて策定）
3.被災時の対処	**① 復旧目標の設定**	優先復旧業務を特定し、復旧目標時期を定め、社内目標として掲げる。
	② 復旧資金の確保	・国、都道府県、市町村の公的支援制度（低利融資、補助金など）を活用する。各種制度の内容について日本政策金融公庫や商工会議所などの相談窓口で情報を得る。 ・加入している保険や共済の保険金などを活用する。
	③ 取引企業との連携	取引企業に状況を伝え、積極的に支援を求める（どのような場合にどのような支援を求めるか、あらかじめ検討しておく。）
	④ 情報の発信	インターネットなどにより対外的な情報発信を実施・継続する。
	⑤ その他	（各社の必要に応じて策定）

- 上記の項目について、実施した事項、実施が必要な事項、検討結果、被災時にとるべき行動などを文書にして、経営者と従業員とで共有することにより共通の認識を形成しておくことが重要。
- 事業継続計画の内容は、事業継続の障害として何を想定するか（地震、水害、事故、新型感染症など）、策定する企業の立地状況や業種、業態、規模、経営戦略、その他の固有の事情に応じて異なるため、上記の他にも企業によって必要な項目があり得る。
- 最新の状況を踏まえて、随時、見直し・再検討・修正を継続していくことが必要。

2. BCPとITサービス継続

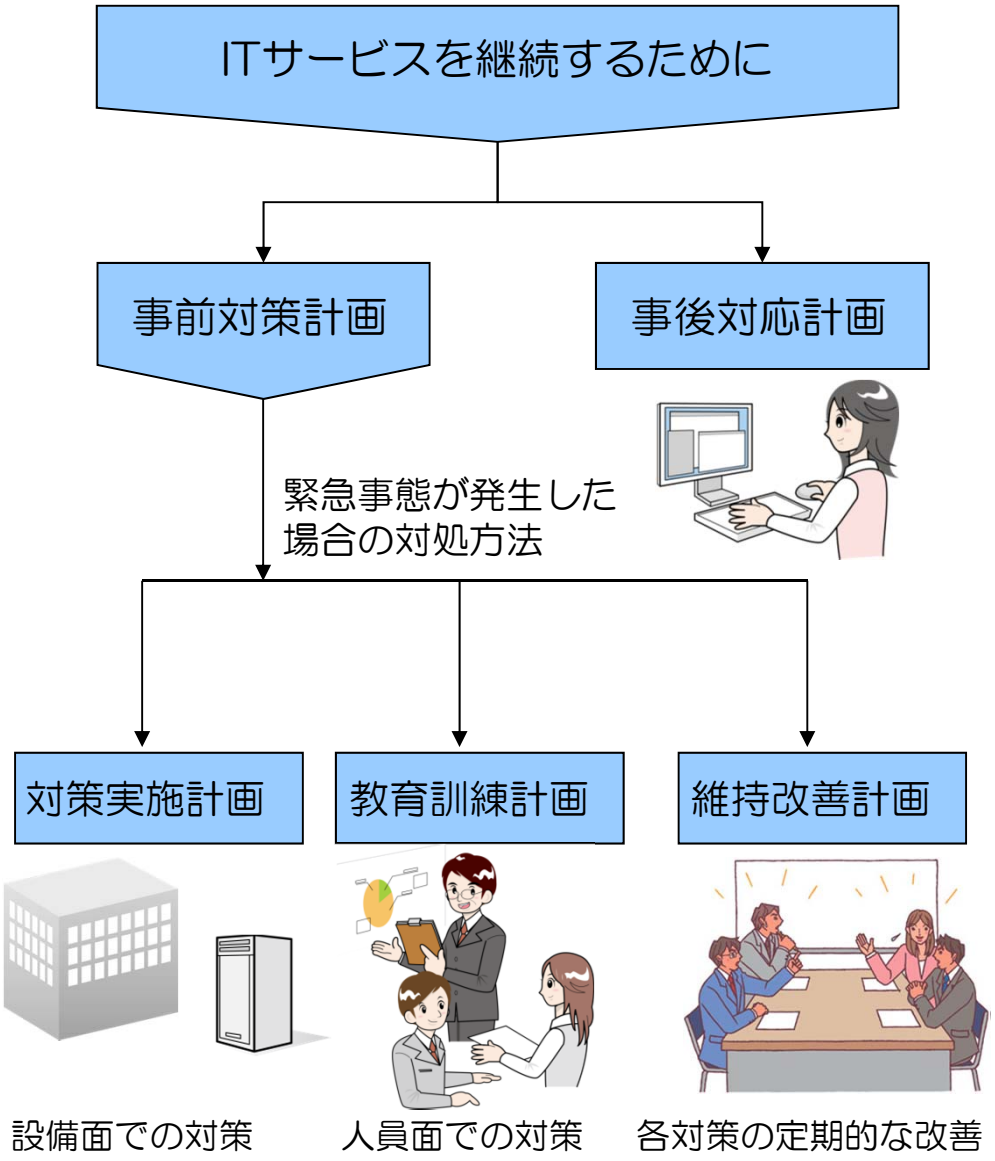
2.1 運用面の対策

(1) 事前対策計画

企業活動にとってITシステムはなくてはならないものとなっており、災害などによりITシステムが長期間停止することは、企業活動に重大な影響を与えます。

BCPにおいて、ITサービスが停止した場合の復旧手順や、停止に陥らないためのリスク対策が必要となります。また、これらの運用方法について、定期的に計画の見直しやメンテナンスが必要になります。

作業ステップ	作業項目	1月	2月	3月	4月	5月	6月
1. BIA調査	アンケートの立案 実施・集計 報告と承認						
2. リスク対策	資料の準備 実施・集計 報告と承認						
3. 継続対策	情報の整理 継続対策の立案 報告と承認						
4. 行動計画	BCPチーム決定 行動計画の立案 マニュアルの立案						
5. BCP文書作成	原稿作成 ドラフト完成						
6. 検証	BCPのテスト 修正と承認 完成(最終成果物)						



⑵ 事後対応計画

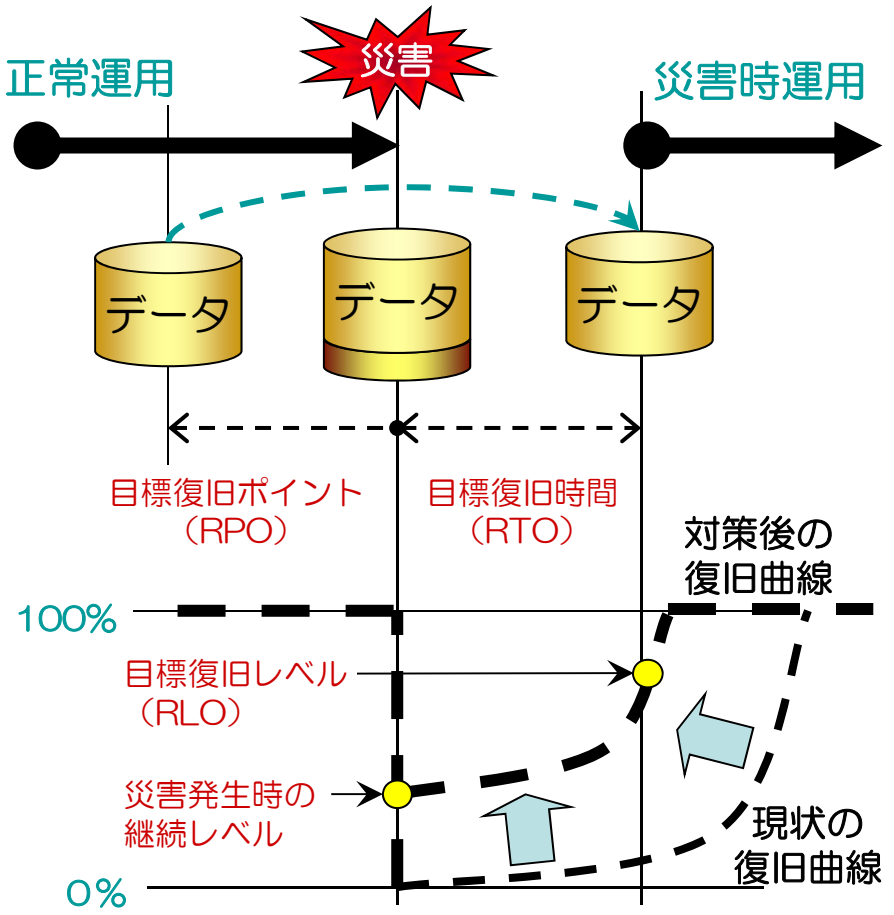
災害が発生し、ITサービスが継続できなくなった場合に備えて、 ITサービスを再開するための手順を準備しておく必要があります。

その準備に当たり、以下の項目を検討します。

- **目標復旧時間（RTO）**
  サービス中断後、復旧までに許された時間
- **目標復旧レベル（RLO）**
  目標復旧時間内に復旧させる操業水準の程度
- **目標復旧ポイント（RPO）**
  目標復旧時間内に復旧させる過去の時点

また、復旧あるいは代替の方法を検討することも重要です。例えば、メールなどはパブリックのクラウドサービスを使うことで、比較的簡単に代替することが可能です。しかし、社内のローカルサーバで動いていたシステムを、全く別のサーバに移行するのは、災害の復旧ではなくても容易ではありません。

あらかじめ仮想環境で動作する、仮想ディスクイメージを用意して、遠隔地に取ったバックアップをインポートするなどの準備が必要です。



例えば、平常時100個／1時間の生産（処理）に対し、ITサービスが停止した時に、
- いつまでに（1日以内など）
- どの操業度（80個/時間など）

という目標を検討します。

2.2 設備面の対策

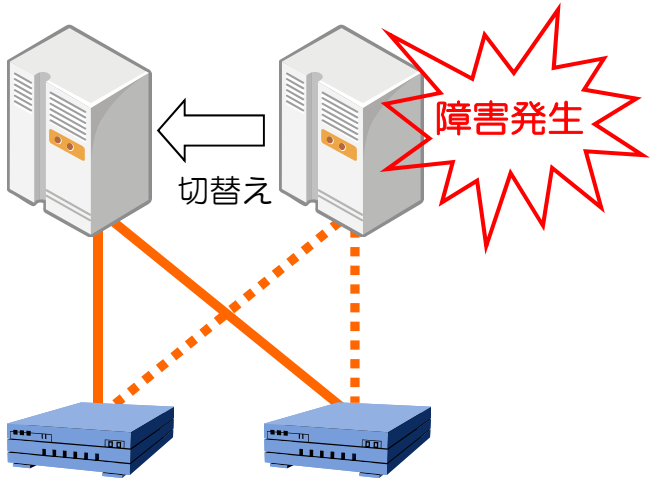
(1) システム二重化

ITシステムを二重化することにより、その一部に障害が発生した場合でも、システム全体として継続稼動を可能にしたり、あるいは目標復旧時間や目標復旧時点をゼロに近づけることができます。

ITシステムやネットワークにかかわるすべての機器を二重化できれば理想的ですが、そのためには膨大なコストが必要となるだけでなく、システム構成が複雑化するという弊害もあります。

ITシステム自体の重要性だけでなく、個々の装置の役割や停止した場合の影響を把握し、コストに見合う範囲で優先度の高い箇所を二重化する、といった対応が必要となります。

この際、直接的なITシステムだけでなく、サーバルームの空調設備や入退室の管理システムなどといった間接的なシステムの停止による影響、あるいは災害や停電などによる大規模なシステム障害の可能性も考慮したうえで、リスクとコストのバランスから対策範囲を決定することが重要です。



ITシステムを二重化することにより、サービス継続が可能となりますが、大きなコストがかかることへの考慮が必要です。

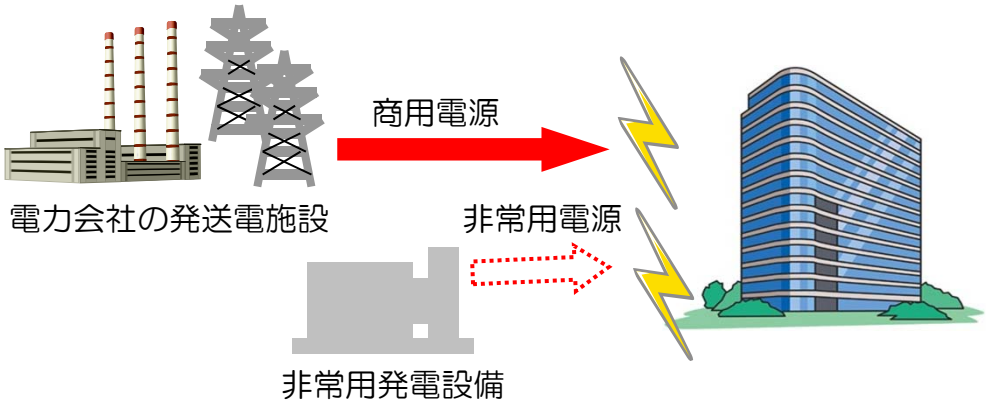
コストに見合う範囲での冗長化の検討が必要ですが、その場合空調設備や、電源などへの対策も考慮する必要があります。

(2) 電源二重化

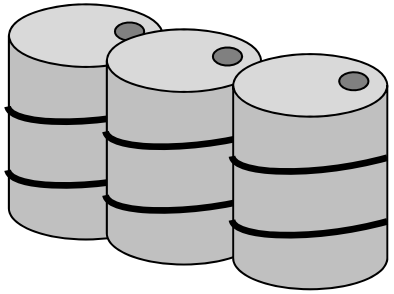
落雷などによる瞬断や停電に対する対策として、安定した電力を供給するUPSがあり、広く普及しています。UPSは、サーバなどを正常に終了させるまでの時間を確保するために使用するものであり、ITシステム機器を継続稼動させるためのものではありません。

ITサービスを継続させるためには、非常用の発電設備を設置して電源系統の二重化を図るのが一般的です。この非常用発電設備は、建物側で設置されているところは少なく、それぞれのITシステムにおいて対策が必要になります。持ち運び可能なタイプから屋外設置型などがあり、供給できる電源容量や稼働時間によって適切なものを準備しておく必要があります。

非常用発電設備はディーゼルエンジンなどによる発電で電力供給を行いますが、運用するにあたって、エンジンを駆動するための燃料を確保しておくことも重要です。特に震災などの非常時には、燃料の確保が困難になることも想定されるため、運用にあたってのリスク面として認識しておく必要があります。



ITサービスの継続には電源系統の二重化を図るのが一般的です。



非常用発電設備の運用には燃料の確実な確保が不可欠です。

(3) 転倒や落下、位置ずれ防止

ITシステム機器の転倒や位置ずれが生じることにより、ITシステムの障害や搭載ラックの損傷、ケーブルの断線などが発生する可能性があります。書庫やロッカーの様な什器に行われる壁面への固定などの簡易的な手法の他、 ITシステム機器搭載ラックに対する免震／耐震対策なども比較的普及しています。これらの対策は、データセンタなどで採用されていることも多く、対策の1つとして高い水準を確保することが可能です。

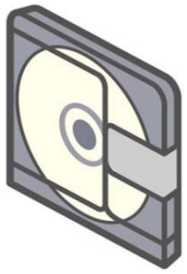
建物自体の対策については、特に1987年（昭和63年）6月以前の旧耐震基準によるものかどうかを確認し、必要に応じて補強工事を実施したり、免震／耐震対策が講じられたビルへの移転を検討する、といったことが考えられます。この場合、システム二重化の対策と同様に、多額の費用を伴う施策領域であるため、経営的な観点でリスクとコストのバランスを考慮した検討が求められます。

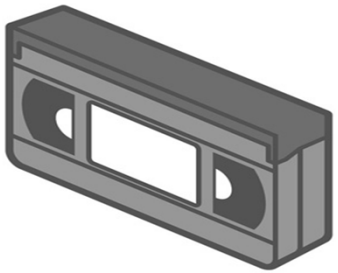
(4) バックアップ

トラブルや災害によって、重要なデータやITシステム自体が被害を受けた際、速やかにそれを復旧するため対策の1つがバックアップです。

企業の規模や業種などにかかわらず、バックアップを一切実施していない、というケースは極めて少ないと考えられますが、事業への影響度を考慮した設計を行い、計画的にバックアップを取得することが重要です。

例えば、更新頻度の高い重要なデータであれば、目標復旧ポイントを直近にするためにできるだけ短い周期でバックアップを行う必要があります。また、目標復旧時間を短縮するために、容易に復旧できるような手段をとることも重要です。





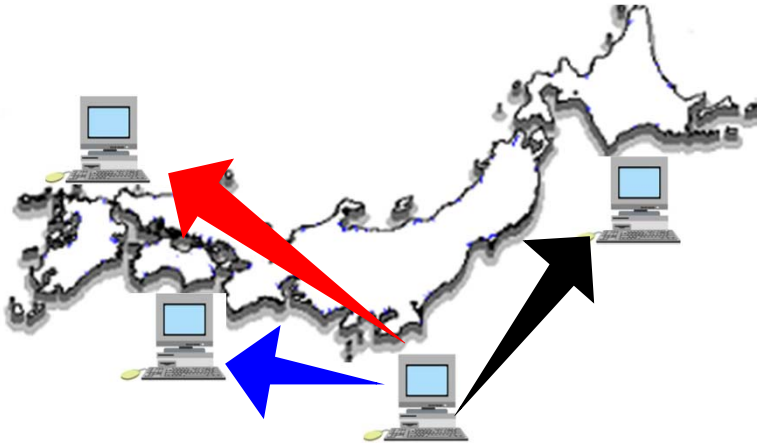
逆に更新頻度の低いデータや、業務アプリケーションなどのITシステム自体をバックアップする場合は、比較的長い周期でバックアップを実施することで十分です。

比較的長期間、データを確実に保存しておくためには、ディスクやテープなどの記録媒体が適していると考えられますが、目標復旧ポイントや目標復旧時間を短縮するためには、外部のサーバやストレージのような媒体への保管と併用することも考慮すべきです。

また、バックアップしたデータの保管場所も重要です。これまでは目標復旧時間を考慮して保管場所までの移動手段や移動時間を中心に検討が行われてきましたが、先の震災のような大規模で広域にわたる災害を想定した場合、遠隔地に保管するのが望ましいと言えます。

このような課題を解決する手段として、ネットワークを経由して他拠点のサーバにデータを保管したり、バックアップサービスなどを利用してデータセンタに保管する方法があります。ただし、これらの方法を利用する場合には、ネットワークが停止した際の復旧方法も考慮しておかなければなりません。

以上の点を踏まえた対策を講じることにより、堅牢で強固なバックアップ対策となります。



バックアップを遠隔地に

ネットワークを利用したバックアップ

2.3 BCP対策としてのクラウド

2011年3月に発生した東日本大震災では、ITシステム自体よりもITシステムの建物や電源などの環境・ファシリティ面における対策の重要性が大きくクローズアップされました。

例えば、数日にわたる停電や計画停電など、これまでのようなUPSを中心とした対策では、とても耐えうるものではありませんでした。さらに、発電設備の準備があっても燃料の提供が制限されるなど、これまでよりも広い範囲での対応策が成されていなければなりません。

また、被災地域が非常に広い範囲であったために、予備的なバックアップサイトも十分に距離をおいた地域にする必要がありました。

そのような背景の中、これらに対応しうるITシステムの対策は非常に大規模・広範囲に行う必要があり、その対策にかかる投資費用も大きくなってきます。また、複数年にわたる対策が必要な場合もあるでしょう。

このため、すでに十分な対策が準備されたデータセンタや、データセンタを活用し提供されているクラウドサービスが大きく見直されています。

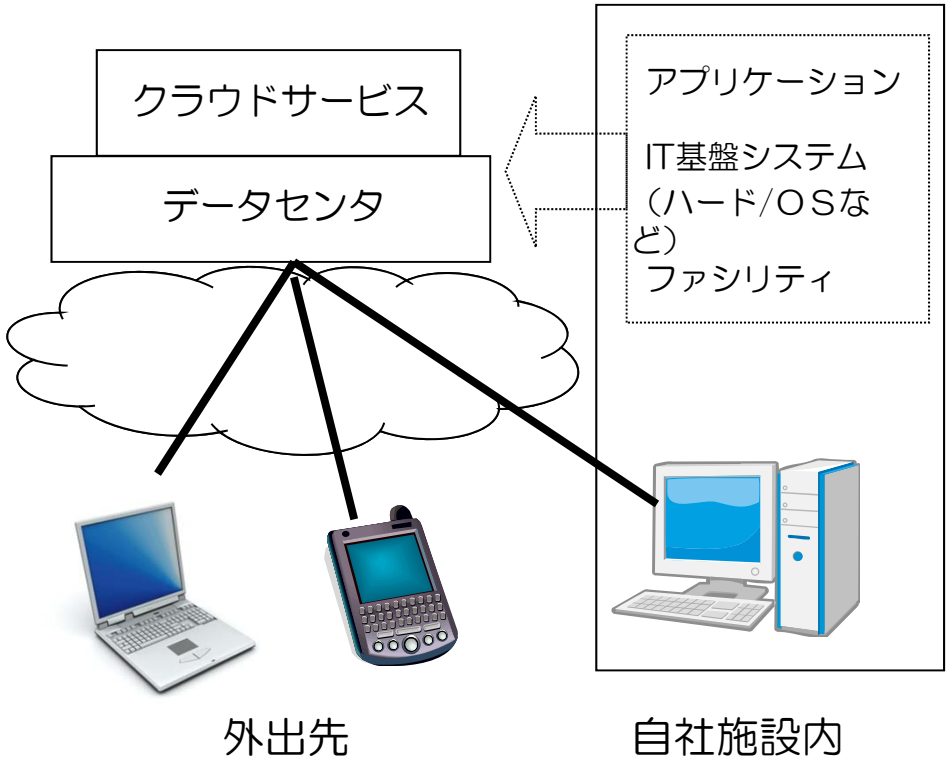
東日本大震災以降、環境・ファシリティ面の対策がクローズアップされています。

災害に強い堅牢なITシステムの対策はコスト・時間がかかります。

現在では数多くのデータセンタやクラウドサービスが提供されており、その競争原理から数年前と比較しても非常に利用しやすい価格帯になってきています。

また、各々のサービスにおける、建物やITシステムが「どれぐらいの耐震環境なのか？」「停電時にどれぐらい連続供給できる電源環境なのか？」などの設備環境面で、その提供価格の差が表れていると考えても良いでしょう。

事業継続計画における、目標復旧時間（RTO）や目標復旧レベル（RLO）などの目標値に基づくITサービス継続性管理に合わせ、自分たちで大規模な災害対策を行う投資額と、それらの条件を持つ「データセンタやクラウドサービスの利用」とを比較・検討をされると良いでしょう。



数多くのデータセンタやクラウドサービスがある中で、
自社の事情や条件に見合うものを選択しましょう。

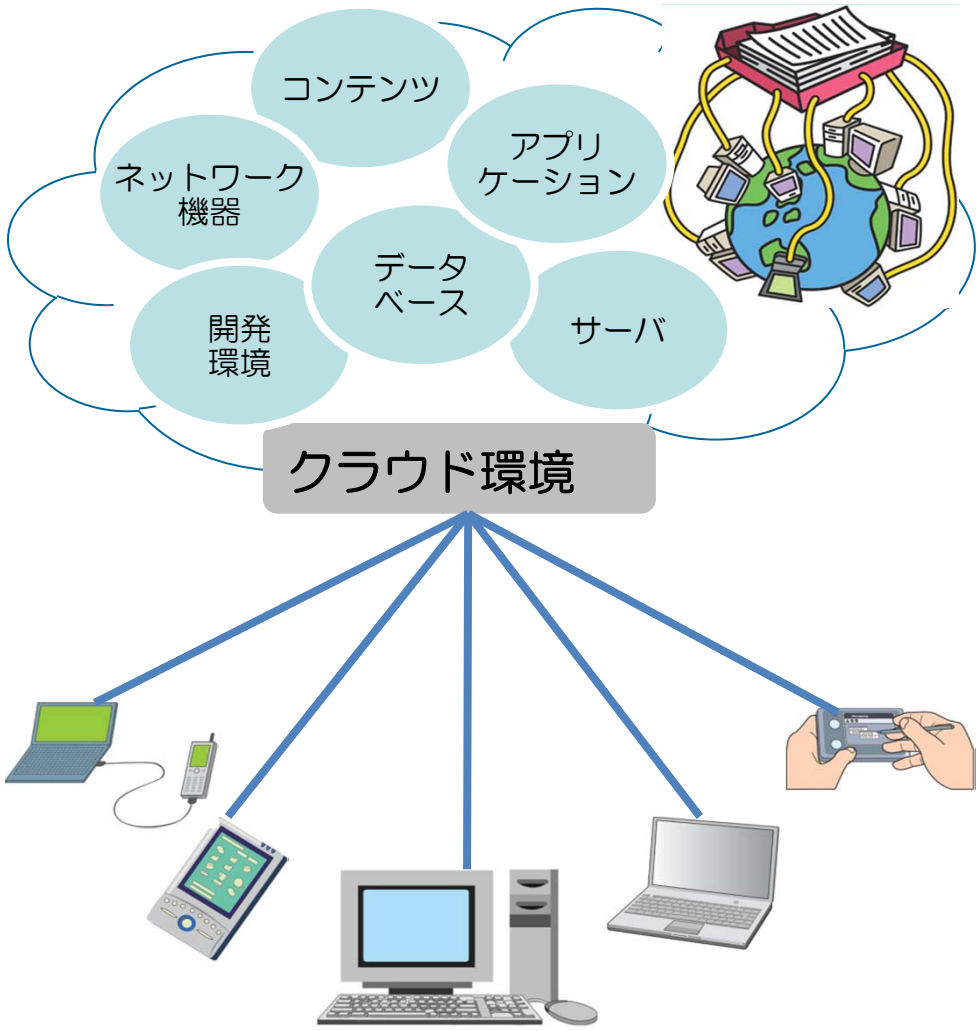
3. クラウドのメリットとリスク

3.1 クラウドサービスについて

クラウドサービスとは、インターネットの先にあるコンピュータに処理を任せる「クラウドコンピューティング」によって提供される情報処理サービスの総称です。以下のような特徴を持つサービスとして登場しました。

従来は、ユーザがコンピュータのハードウェア、ソフトウェア、データなどを自分自身で保有・管理していたのに対し、クラウドサービスにおいては、利用者は最低限の環境（PCなどのクライアントとブラウザ、インターネット接続環境など）のみを用意し、利用したサービスに応じた料金を支払う形態となります。

自社にシステムを構築する場合と比較して、初期投資を抑え、システムの利用開始までの期間を短縮できる上に、セキュリティパッチをはじめとするOSやアプリケーションの更新作業、ユーザなどの増加に伴うシステム拡張への対応もサービス提供事業者にお任せできるなど、運用面でもメリットがあり、TCOの削減やビジネスのスピードアップといった効果が期待されます。



クラウドの中のしくみを気にせず、必要に応じてさまざまなサービスを利用することができます

3.2 クラウドサービスの種類と特徴

その後、1企業が部門サーバの統合、グループ内のサービス統合をクラウド型で処理する形態が現れ、いくつかの種類に分かれてきました。

(1) パブリッククラウド（Public Cloud）

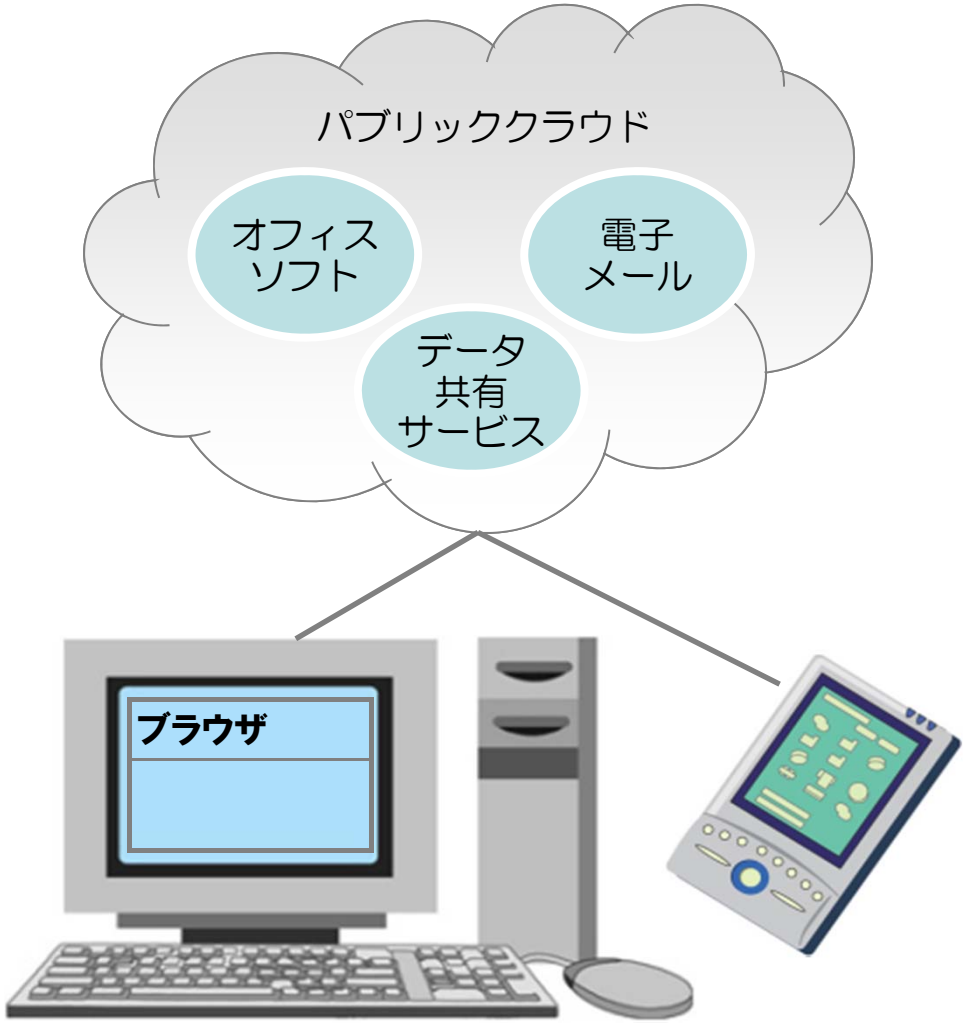
パブリッククラウドとは、データセンタ事業者などが、広く一般の利用者に提供するクラウドコンピューティング環境のことです。

特に中小企業においては、主に社内で利用しているシステムやソフトウェアをクラウドサービスに移行するという形で利用されています。また、企業が外部向けのサービスを提供する際の基盤としても利用されています。新たなサービスを始める場合など、最小限のリソースのみ契約する「スモールスタート」により、初期投資や運用コストの抑制が可能です。

無料プランや安価なプランが用意されている反面、安定性やセキュリティ面での対応レベルはサービスベンダに依存するため、慎重な選択が必要です。

このパブリッククラウドの対義語となるのが「プライベートクラウド」（Private Cloud）ですが、これは主に企業などが社員や関係会社など内部の

利用者に向けて提供するクラウド環境のことをさします。次頁で詳しくご紹介します。



クライアントマシン
の性能に依存しない

(2) プライベートクラウド（Private Cloud）

プライベートクラウドとは、企業が自社内でクラウドコンピューティングのシステムを構築し、企業内の部門やグループ会社などに対してクラウドサービスを提供するための環境です。限られた場所や限られたネットワークからのアクセスのみ許可されるようになっています。

主に大企業においては、自社システムの補完や補強の手段として利用されているケースが多く、短期間の大容量データ処理や、時期によって負荷の変動する処理だけを、クラウドに移行するという活用方法や、コストメリットの出やすい部分だけを移行するといった形で活用されています。

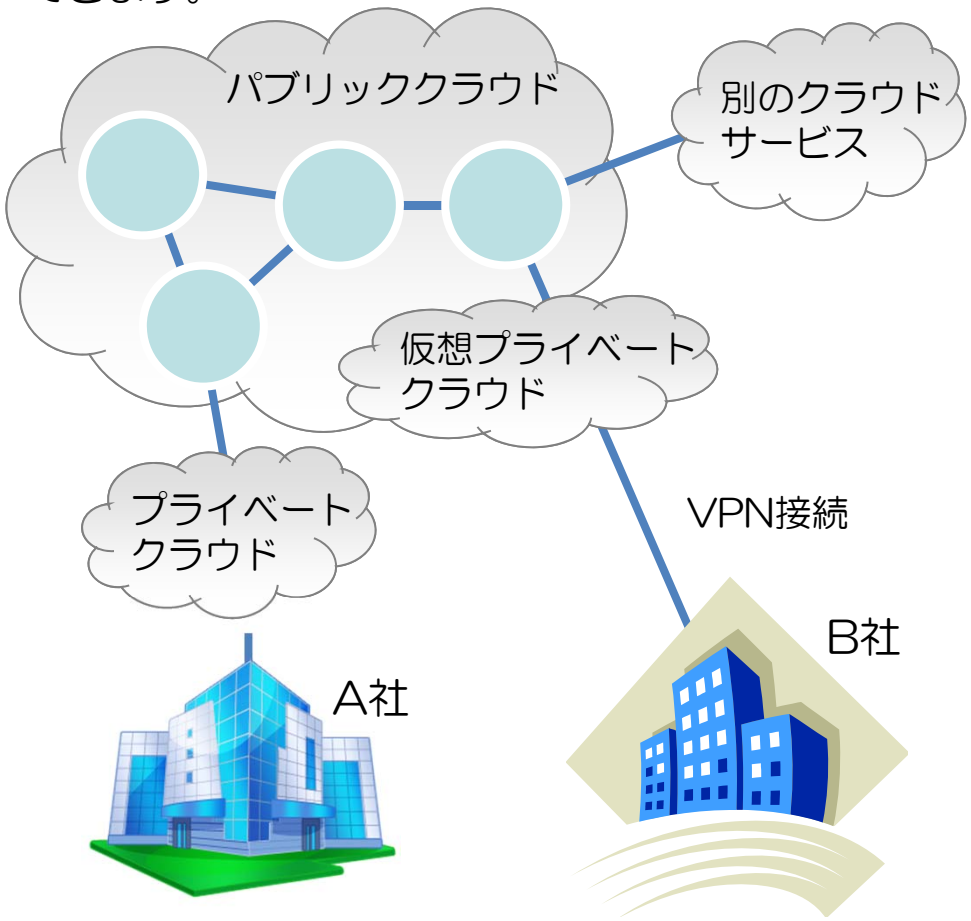
システムのどの部分を自社で運用し、どの部分をクラウドに移行するのか、その範囲を正しく見極めることが重要です。

クローズドなシステムとなるため、パブリックなクラウドサービスに比べて企業内のセキュリティポリシーの実現が図りやすいといった面は、パブリッククラウドには実現できないメリットの1つです。

(3) ハイブリッドクラウド（Hybrid Cloud）

パブリッククラウドとプライベートクラウドを組み合わせたクラウドサービスのことです。

2種類のクラウドサービスを特性に応じて使い分け、それぞれのメリットを最大限に引き出すことができます。



3.3 クラウド新サービスの拡がり

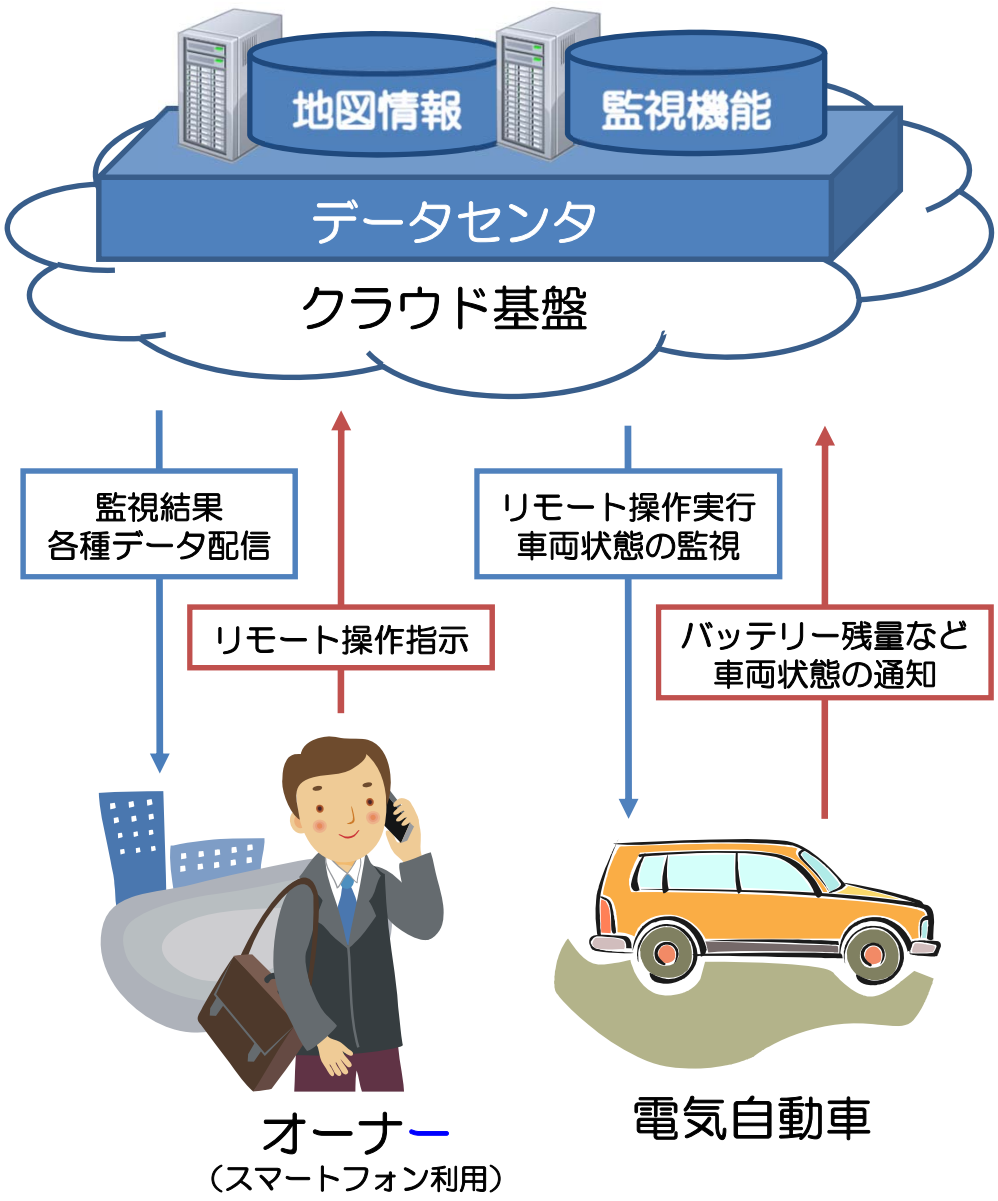
現在、市場にはクラウドコンピューティングのスケールメリットを活かした新サービスが続々と登場しています。その活用範囲は、自動車産業に加えて医療、社会基盤に至るまでさまざまです。

(1) 自動車クラウド

クラウドサービスを利用した次世代自動車が注目を集めています。

自動車業界では、電気自動車などにクラウド技術を活用し、データセンタと連携させることによって、カーナビに高機能なプロセッサを搭載せずとも、高度な処理を可能にしました。

従来とは異なり、データ管理以外の処理もクラウド側で行うことで利用時のスピード感が向上しています。走行履歴や渋滞状況、エネルギー残量に応じた充電設備まで、多様な情報をクラウドで処理してオーナーへ配信します。



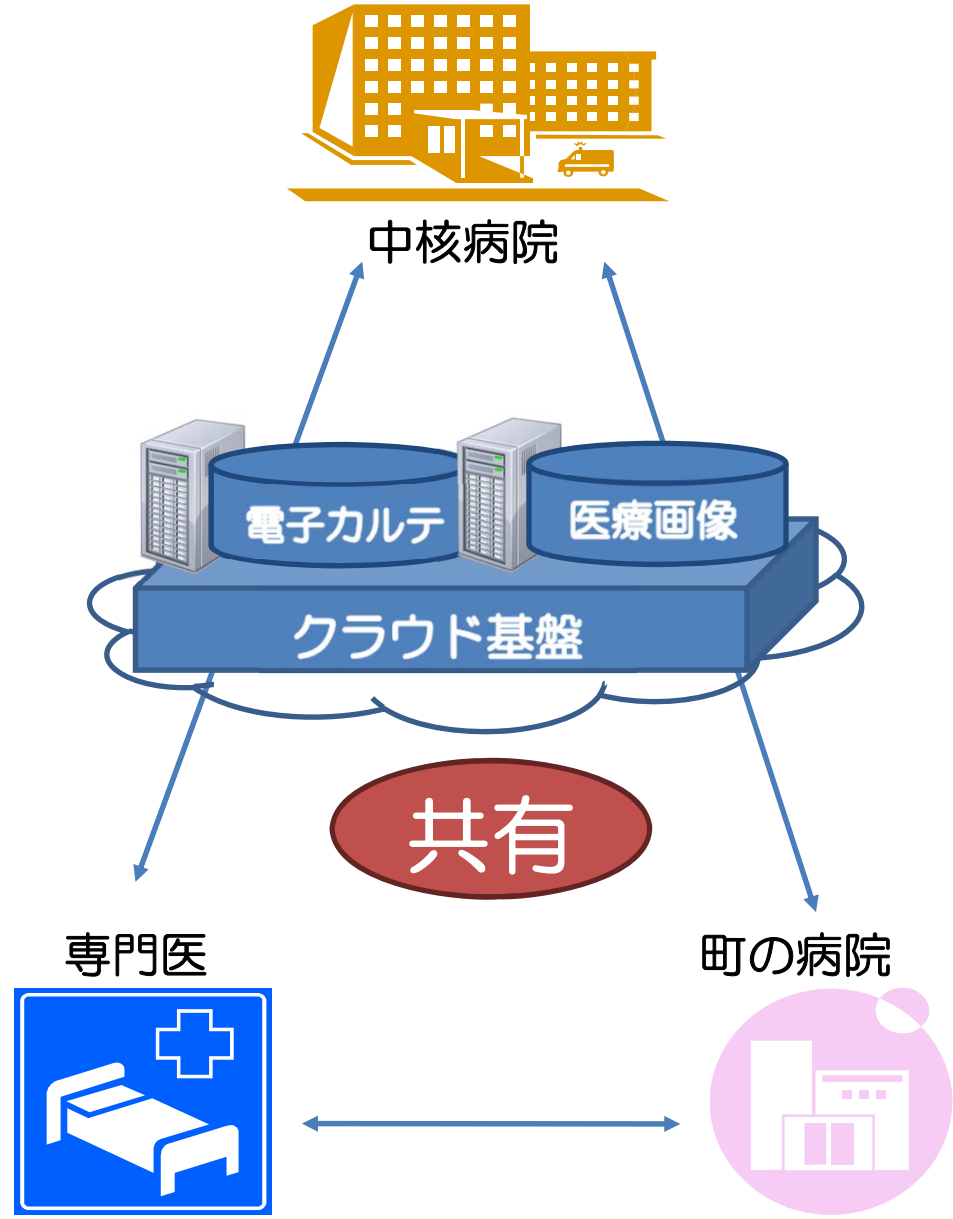
(2) 医療クラウド

電子カルテシステムが推進されている現在、そこから一歩踏み込んだ医療クラウドが浸透し始めています。

医療クラウドとは、患者の情報をクラウド上で一元管理することにより、ネットワークを経由して各所での利用を可能にしたサービスです。利便性の向上と共に、大量の医療画像データを管理する手間を削減できるメリットがあります。

さらに今後、電子カルテの普及次第では病院間をつなぐクラウドサービスも実現されつつあります。街の中核病院、町の病院、専門医の三者がクラウドを通じて電子カルテを共有できれば、過去の病歴や投薬歴に基づく、より適切な医療を提供することが可能となります。

情報の堅牢性や法制度などの問題はありますが、医療クラウドは将来を期待される分野の1つです。



⑶ M2M型クラウド

クラウドの活用は新規ビジネスのみにとどまらず、社会基盤の分野でも大きな貢献を果たしています。その代表例が、M2M（マシン･ツー･マシン）型クラウドという、人を介さず機器同士のデータ通信を行うシステムです。

現在、世界各地でスマートシティ関連の構想が数多く推進されています。スマートシティとは、エネルギーや交通の管理をIT技術を用いて都市全体で効率よく運用する、次世代環境都市のことです。

この構想の中核にはスマートグリッド（次世代通信網）という技術があり、M2M型クラウドはそのインフラを支えています。仕組みとしてはまず、各家庭や工場、発電所などにスマートメーターを設置します。そして、収集したエネルギー使用量などのデータに基づいて機器の制御を行い、無駄のない運用を目指します。

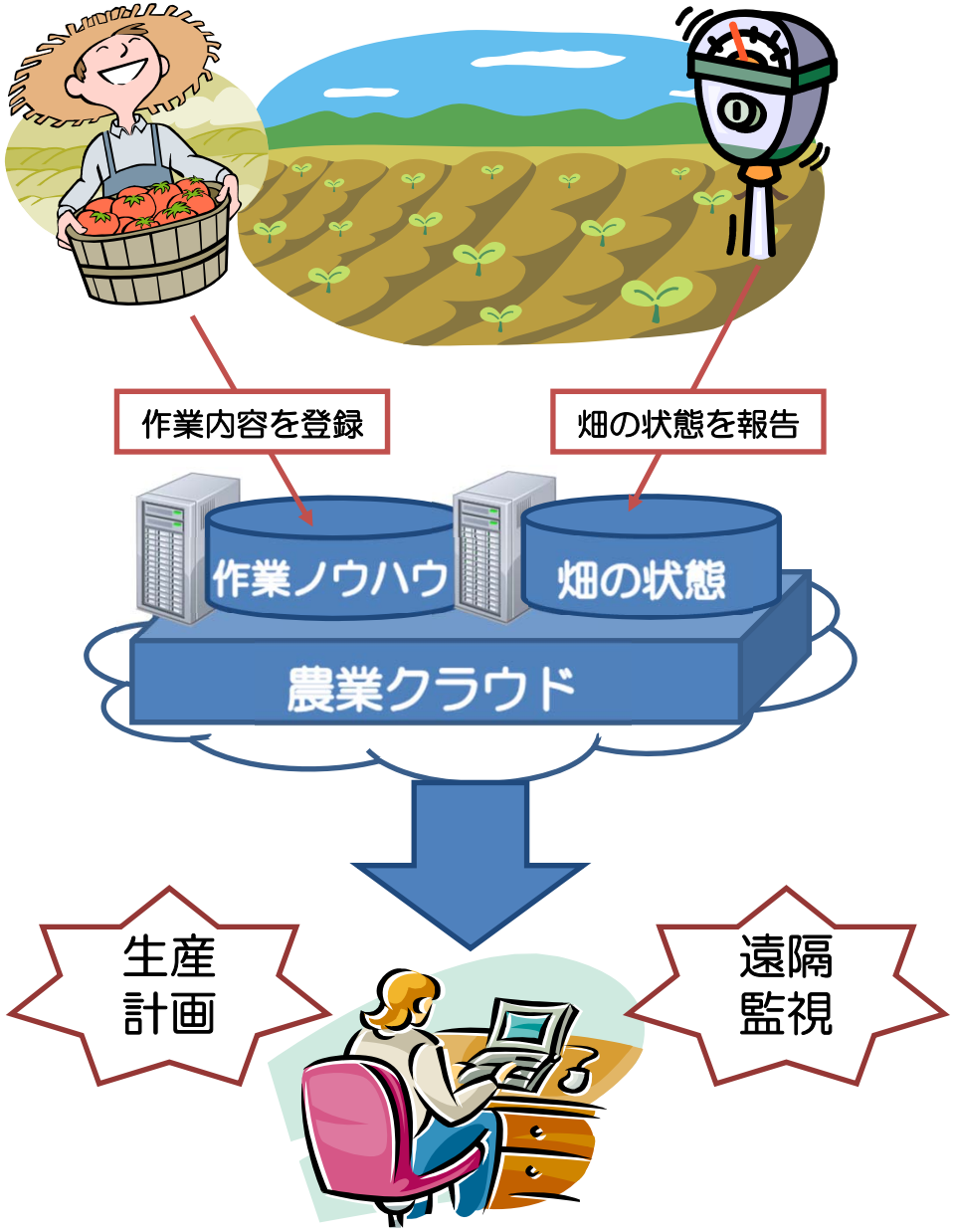
M2M型クラウドによって今後、さらに多くの都市機能が連携し、人々の生活が豊かになることが期待されています。

(4) 農業クラウド

従来、農業はITの導入があまり進んでいない分野でした。しかし近年、業界全体で資源を共有するクラウドならば、コストを低く抑えたIT化が可能だとして、農業クラウドの実験が進んでいます。

畑の遠隔監視では、地中にセンサーを埋め込み、温度や水分、気温などの状態を計測し、ウェブカメラで撮影した映像と共に、クラウド上のシステムへ送ります。それにより、農家は直接畑へ行かなくとも状態を監視することが可能になります。

さらに、ベテラン農家が培った勘や経験を、広く共有するために開発された仕組みが、農作業管理システムです。作業時間や内容、場所をクラウド上に登録することでノウハウを蓄積し、生産スケジュールの計画へと活かされています。



3.4 クラウド移行に際して考慮すべき点

クラウドを利用する際の懸念事項としてよく取り上げられるものに、セキュリティ（情報漏洩のリスク）、安定性（サービスや情報の可用性）、コストの3点があります。ここでは、それぞれの考え方について述べていきます。

(1) セキュリティに関する懸念

クラウドサービスを利用する際、セキュリティに対する不安の声がよく聞かれますが、その多くは、明確な懸念ではなく漠然とした不安のようです。

当然ながら、クラウド事業者では、ウイルス対策や不正侵入対策などの外部からの攻撃対策に加え、アクセス制御や変更管理などの内部的なリスク対策など、さまざまなセキュリティ対策を一般の企業よりも高いレベルで実施しています。従って、クラウドへ移行することで、すぐさまセキュリティ面でのリスクが高まることはありませんが、事故などによってクラウドサービスで利用するデータが漏洩するリスクについては、十分に考慮しておく必要があります。

機密性の低い情報を扱うサービスの場合には、セキュリティ面のリスクはそれほど気にかける必要はありませんが、顧客情報や企業機密にかかわるような重要なデータを取り扱う場合には、事業者の責任範囲と対策の概要を把握しておく必要があります。特に、ほかのユーザが重要なデータへアクセスすることを制限、監視するためのアクセス制御や、万一データが流出した場合の実被害を抑制する暗号化などの対策状況や管理方針を確認しておきましょう。

セキュリティ対策にかかわる詳細情報は、それを悪用されるリスクにもつながるため、事業者側もあまり多くの情報は開示していません。また、それを入手できた場合も、対策内容が妥当なものかを判断することは容易ではありませんが、事業者と利用者との間で、情報が漏洩した場合のリスクについての認識を揃え、双方の責任を理解した上で正しく利用することが重要です。

(2) サービスの安定性

クラウドサービスを利用する際、障害やメンテナンスなどの影響によって、サービス自体が利用できない状態や、重要なデータにアクセスできない状態が発生することが考えられます。

クラウド事業者側でも、データのバックアップ、システムの分散、冗長化などによって、サービスの継続性、安定性を高めるような設計、運用を行っていますが、障害発生のリスクをゼロにすることは不可能です。そのため、多くの事業者では、SLA（Service Level Agreement）やSLO（Service Level Objective）といった形で、サービス継続性に関する想定品質を規定しています。これらは一般に公開されていない場合もありますが、サービスを利用する際には、これらの情報を事業者に確認することが重要です。

障害は起こりえるものと想定し、サービスが停止した場合の影響を考慮し、期待する品質を明確にしておく必要があります。しかし、期待する品質を定義しても、自社内でその品質を満たすためのシステム設計や運用を行うことは容易ではないため、過剰な投資を行ってしまうケースが多く見られます。

一方クラウドサービスでは、事業者から提示される情報を元に、そのサービスが期待する品質か否かを判断することが比較的容易に行えます。また、災害対策の観点から見ても、自社内で運用する場合と比較し、遠隔地で運用されるクラウドサービスの方が高い効果を期待できます。

サービス安定性にかかわるリスクはクラウド特有のものではないことを認識した上で、それぞれのサービス品質を十分に確認し、期待するサービスレベルを満たすものを選択することが重要です。

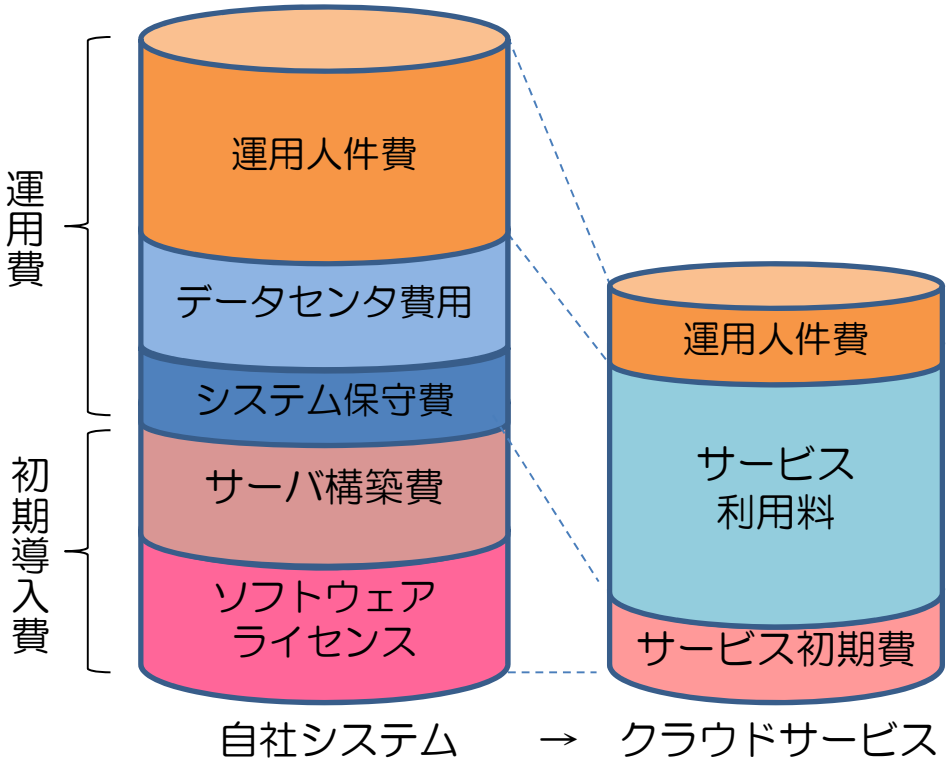
(3) クラウドとコスト

サービスの安定性を高めるためには、事業者の提供コストも高くなり、安定性を重視しないサービスでは提供コストも低くなります。類似するサービスであっても、サービスの品質レベルや付加価値によって、適正なサービス料金も異なります。コストを比較する際は、自社にとって必要な要件を満たすものを、相対的に比較する必要があります。

クラウドサービスの利用料金を一般的なソフトウェアのライセンスと比較した場合、クラウドの方が割高に見えるケースが多くあります。しかし、ハードウェアのコスト、データセンタ利用料や電力などを含めた設置コスト、導入や運用にかかわる人件費など、付帯的なコストを含めて考慮すると、一般的にはクラウドサービスを利用した方が割安になるケースが多くなります。

しかも、クラウドサービスの方が導入にかかわる初期費用を低く抑えられるケースが多いため、比較的短期間で投資の回収を行える、試験的な導入を実施しやすいといったメリットも挙げられます。また、クラウドサービスの多くは、従量制の課金体系をとっており、利用者は実際の利用量に応じた費用を支払うことになります。このことにより、需要の変動を考慮して事前に過剰な設備投資を行う必要がないだけでなく、キャパシティ管理の手間や設備増設に伴う作業負担を減らすという効果も期待されるため、需要変動の大きいシステムでは、特に大きなコスト削減効果が期待できます。

以上のように、クラウドサービスを利用した場合のコストに関しては、一般的にリスクよりもメリットの方が大きくなります。

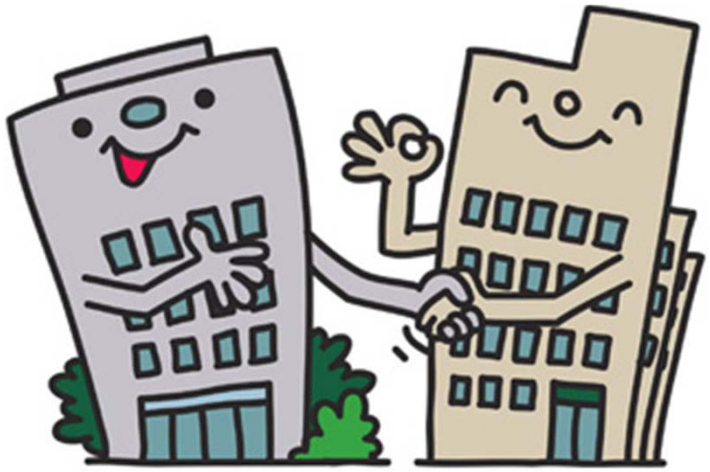


3.5 事業者選定のポイント

クラウドサービスを導入する際には、事業者が開示している情報をしっかり確認し、機能面と信頼性の双方に関して、自社の要件に沿っているかを確認し、選定することが重要です。選定に当たって、事前に確認しておくべき主なポイントをまとめます。

(1) 事業者の信頼性

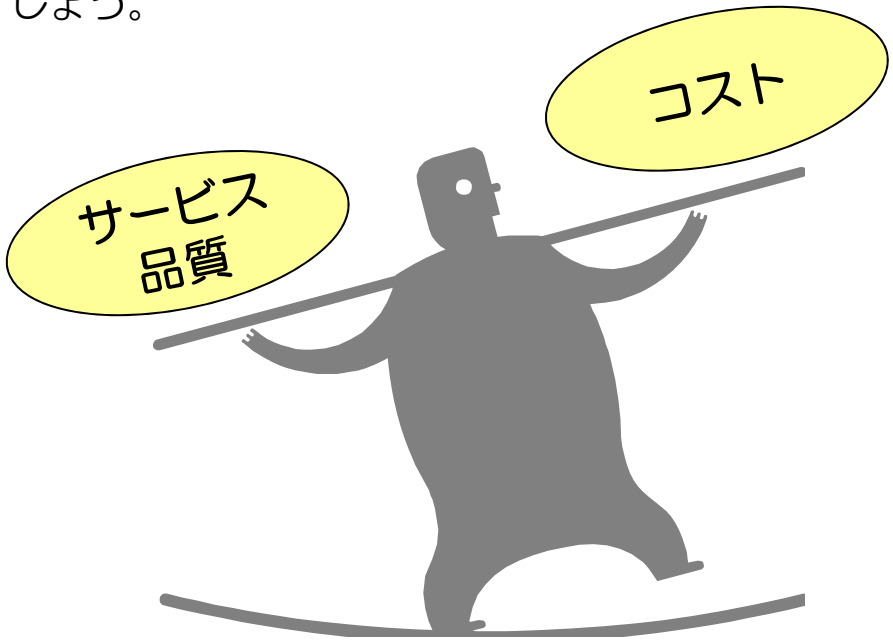
これから導入しようとしているサービスが、突然終了してしまうというリスクを避けるためにも、資金・経営状態や社会的信用など、会社自体の健全性と共に、事業方針や事業体制など、その事業の継続性に懸念はないかを確認しましょう。



(2) サービスの信頼性

SLA/SLOを確認しましょう。特にサービスの継続性にかかわる情報は重要です。情報の開示が少なく、問合せても満足に回答できないような事業者には注意が必要です。また、仮に稼働率99.5%と想定されていれば、1カ月あたり3時間程度はサービスが停止する可能性があると見込んで判断するべきです。

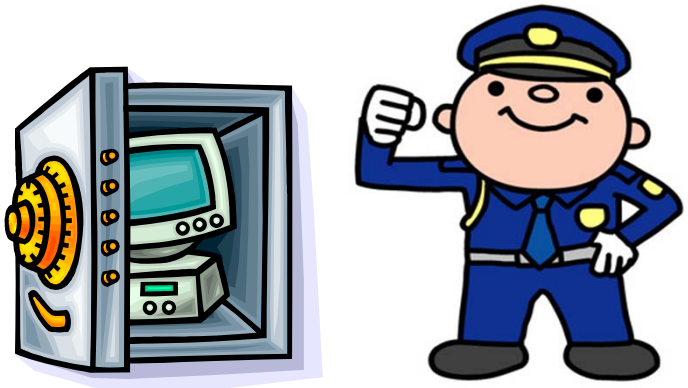
しかし、闇雲に高いサービスレベルを要求すれば当然コストは高くなります。本当に必要なサービスレベルを明確にし、それを満たすものを選択しましょう。



(3) セキュリティ対策

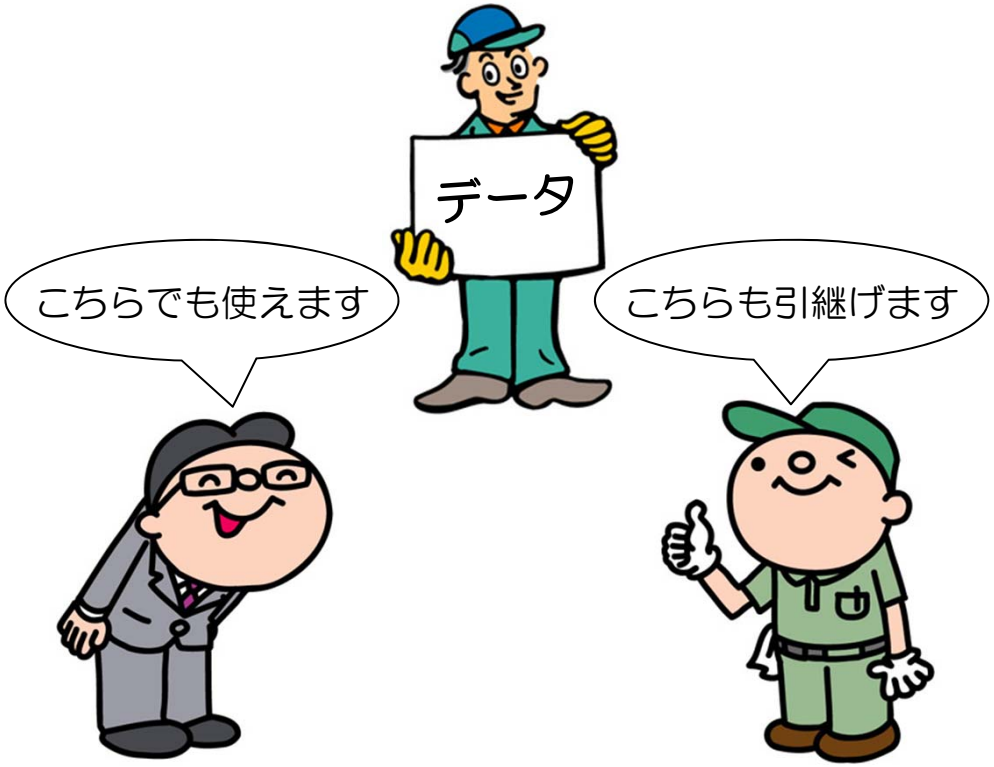
「3.4 (1)セキュリティに対する懸念」で述べた通り、セキュリティにかかわる詳細情報の入手は困難ですが、プライバシーマークなどの公的認証の取得有無、情報取り扱い環境などのセキュリティポリシーの公開有無、セキュリティ監査実施状況などを確認し比較することで、事業者のセキュリティに対する取り組み状況を相対的に把握することが可能です。

技術的に詳しい方であれば、例として監査ログに記録される情報例の提示を求めると良いでしょう。誰が、いつ、どんな操作を行い、どの情報に変更を加えたかなど、預けた情報の管理に必要な情報がどのようなレベルで記載されているかを把握することは、事業者の管理レベルを把握する目安となる上に、問題が発生した際の対応も取りやすくなります。



(4) サービスの依存性

システム運用や管理を事業者に一任することになるため、ほかの事業者への移行が困難な状態（ベンダーロックイン）に陥ることが考えられます。特に、解約時やサービス終了の際に、蓄積されたデータが利用できないようでは致命的な状況に陥りかねません。データをほかのサービスに移行することができるか、互換性や汎用性を考慮したシステムとなっているかを確認しておくことが望ましいでしょう。



(5) その他

(1)～(4)以外にも考慮しておくべき点がいくつかあります。例えば、一般的なサービスと同様に、契約約款に不利な条項が盛り込まれていないかを確認することに加え、クラウド特有のポイントとして、日本でサービス提供されている場合でも、システムの運用や事業者の企業活動は海外で行われている場合もあるため、裁判管轄国を確認し、どのような法制度が適用されるかを把握しておくことが望ましいでしょう。

また、ISMS（ISO27001）、ITSMS（ISO20000）などの第三者保証の保有有無によって、事業者から得られる情報の信頼性を判断する材料にもなります。

クラウドを利用する際に、ユーザ側で考慮すべき点は、経済産業省から公開されている「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」*に体系的にまとめられています。更に詳細な情報を知りたい方は、是非一読されることをお勧めいたします。

---

*:下記URL参照
http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

これまでに述べてきたような情報を把握、理解したうえでサービスを選定することは難しいのではないか、と言う印象を持たれた方も多いのではないかと思います。そのような場合には、利用者がサービスの比較・評価・選択を容易にできるようにすることを目的とした認定制度が助けとなります。

国内では、総務省による情報開示やセキュリティ対策のガイドラインをベースに、安全・信頼性に係る情報開示基準を満たすサービスを認定した「ASP・SaaS安全・信頼性に係る情報開示認定制度」などを目安とすると良いでしょう。

3.6 クラウド化が有効な経営課題

クラウド化はコストの削減に関心が向きがちですが、それだけではありません。利用方法によっては、そのほかの課題に対しても有効な解決手段になり得ます。

(1) グリーンIT

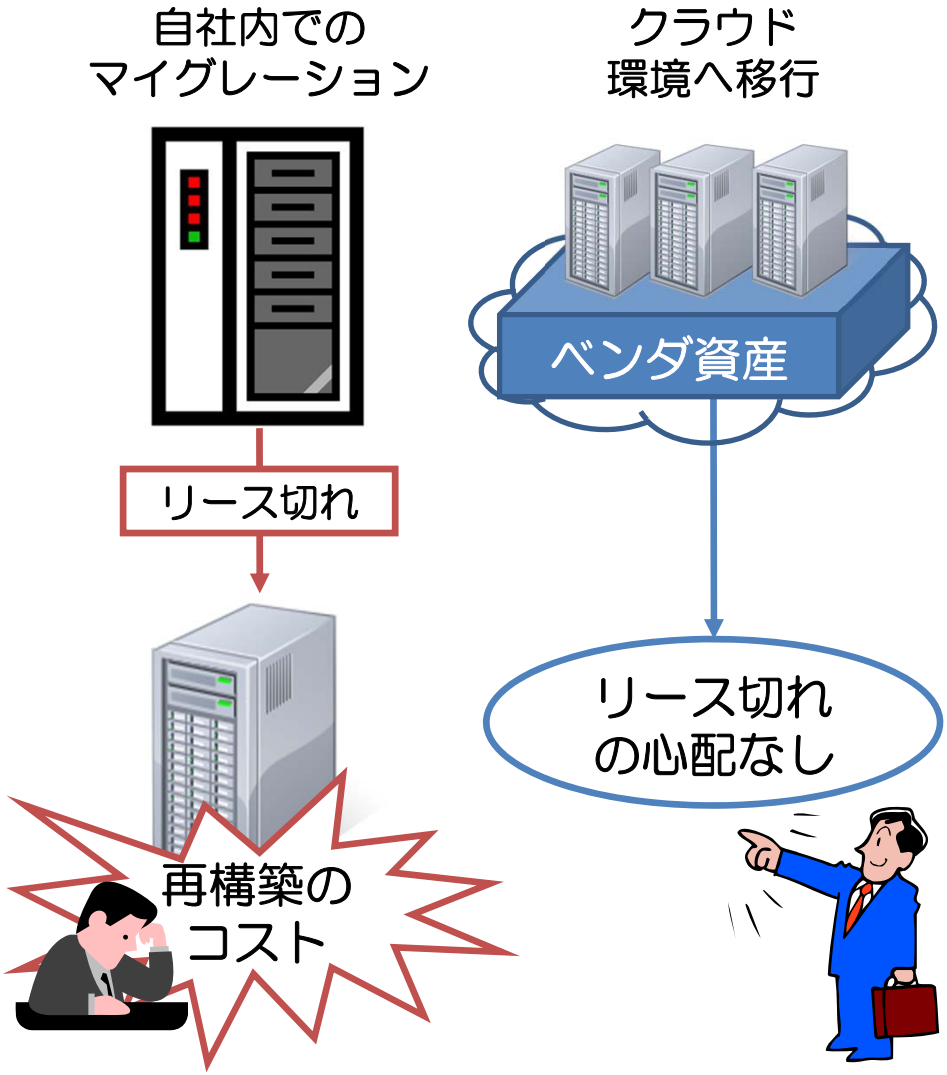
クラウド基盤（ブレードサーバなど）への統合により、大幅な省電力化・設置スペースの削減が期待できます。

(2) プラットフォームマイグレーション

プラットフォームマイグレーションとは、企業の基幹システムを新しい基盤へと切り替えることです。

従来はシステムの保守／サポートの期限を1つの契機として構築しなおしてきました。最近、クラウド化が進むにつれて、従来型の環境からクラウド環境へ移行を決断する企業が増えてきています。ベンダの資産を利用するパブリッククラウドへ移行した場合、企業は長年悩まされてきたハードウェアの老朽化対策という課題から開放されます。

移行に伴う問題ももちろん存在しますが、クラウド化を検討する流れはベンダの後押しもあり活発化しています。



プラットフォームマイグレーションイメージ

あとがき

BCPとクラウド、一見関係のなさそうな言葉に思えますが、大災害によって企業の設備までもが被災した場合、それでも事業を継続するための対策としてクラウドが注目されてきています。まだ、セキュリティ面やデータセンタの設置場所（国内か、海外か）などの面から導入に踏み切れない企業もあると聞きますが、クラウドへの流れは確実に近づいているように思えます。

クラウドサービスを、業務の集中化として利用し、効率を狙う方法もありますが、反面タイの洪水に見られるように、集中化したために災害時、影響が甚大になることを考えると、やはり各企業内の色々なシステムの重要性を考慮しながら適用を判断していくことが大切になります。

これからは、クラウドをどう使っていくか、何を取り入れて何をやらないのか、企業の選択肢の1つとしてその導入の検討を行い、対応していく必要があるでしょう。

サポートサービス委員会事務局

本書は下記の方々のご協力により作成しました。

氏名	所属
伴野　浩之	日本事務器株式会社
芳賀　明夫	株式会社大塚商会
前場　宏之	トレンドマイクロ株式会社
松田　利昭	東芝情報機器株式会社
赤尾　光男	日本事務器株式会社
黒木　直樹	トレンドマイクロ株式会社
平　　玲子	リコーテクノシステムズ株式会社
森　　恭志	株式会社富士通エフサス
森　　達矢	ＮＥＣフィールディング株式会社
吉村　秀樹	株式会社シー・シー・ダブル
佐藤　昭博	
岩崎　透	
加藤　誠	一般社団法人 日本コンピュータシステム販売店協会

ＢＣＰの対策として
クラウドをどう活用できるのか

発行　一般社団法人 日本コンピュータシステム販売店協会
東京都文京区湯島１－９－４　鴨原ビル２階
電話 03-5802-3198
ホームページ　http://www.jcssa.or.jp
発行日　平成24年３月（初版）

© 一般社団法人 日本コンピュータシステム販売店協会 2012

JCSSA