これからのレジリエンシーを支えるメソッドとテクノロジー

～多様化・複雑化するITリスクへのチャレンジ～

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・
サービス事業本部
レジリエンシー・サービス
営業部　部長
高瀬 正子

クラウド、モバイル、Internet of Things（以下、IoT）などの普及により、企業のIT環境は多様化、複雑化が進み、それに伴い事業継続に十分に取り組むことが困難になっている。本資料では、近年のIT環境の状況を踏まえ、レジリエンシーに必要な視点、IBMが考える事業継続フレームワーク、IBMが提供するレジリエンシー・サービスを紹介することで、企業が直面している事業継続の課題の解決に必要なポイントについて解説する。

お客様調査レポートより

IBMは世界のエグゼクティブを対象としたアンケートを実施し、その結果をグローバル経営層スタディとして発表している。その2015年版では経営者の最大の関心事としてテクノロジーが1位となっている。テクノロジーは2012年から1位に選ばれるようになったが、それ以前とはテクノロジーに求められる役割が変わっている。2004～2005年ごろはテクノロジーといえばコスト削減の手段としてとらえられていたが、2012年以降は企業の成長を後押しすることが求められるようになった。つまり、企業が成長するためには顧客を知ることが必要なので、モバイル・デバイスや各種センサーなどを活用して顧客にリーチすることが重要だということだ。その裏付けとして、特に重要となるテクノロジーとしては「クラウド・コンピューティング／サービス」「モバイル・ソリューション」「モノのインターネット（IoT）」が上位を占めている。この3つのテクノロジーの共通点を考えると、スピードが浮かび上がる。モバイル・アプリケーションで1年に1度しかバージョンアップされないというようなものは使われない。そしてスピードを上げるためには、クラウドのように他者のものを借りて使うといった発想が必要となる。こうした傾向は多様化、複雑化につながるものであり、事業継続の考え方にも大きな影響を与えることになる。つまり、自社内のシステムに加え、クラウドなどの外部リソースやモバイル環境、あるいは各種センサーの存在まで広範囲にわたって事業継続を考えなければならない。こうしたIT環境の中でいかにサービスを継続するか、そしてITセキュリティー対策をいかに施すのかということが事業継続のテーマとなるのだ。

次に海外に目を向けてみよう。米国とカナダの19業種の事業継続（Business Continuity：BC）および災害対策（Disaster Recovery：DR）の専門家310名を対象にIBMが実施した調査では、事業継続および災害対策の専門家が直面している課題のトップ3に「ますます増加するビジネス上重要なシステムをBC/DR計画に組み込む必要性」「サイバー・セキュリティー・リスクへの対応」「IT統合拡大により、BC/DRチームが管理対象とする潜在的な障害ポイントの増加」が挙げられている。先に指摘した通り、経営者はテクノロジーにビジネス成長を後押しする役割を求めているので、その分ビジネス上重要なシステムが増加する傾向にある。そこでそれらのシステムをBC/DR計画に組み込むことが課題となっているのだ。つまり事業継続や災害対策が企業の売り上げ向上やブランド価値の維持、企業の信頼性に大きくかかわっているということができる。

またサイバー・セキュリティー・リスクに関しては、次々と新しいサイバー攻撃が登場している昨今では当然のように重視される課題であるといえる。さらにIT環境が自社内にとどまらず多様化、複雑化が進む状況ではそれだけ潜在的な障害ポイントが増えることになる。外部リソースやモバイル環境などとの連携が広がることにより、障害の原因となるポイントを切り分けることが困難になり潜在化する傾向にあるので、その対策が大きな課題として注目されている。

このようにIT環境が多様化、複雑化する状況において、自社のITインフラへの事業継続、災害対策の準備ができている企業がどのぐらいあるのであろうか。IBMの調査結果では準備ができていると回答した企業は全体の10%以下にとどまっている。つまり90%以上の企業が、災害などが発生した際の事業継続対応は難しいと考えているのだ。その理由として、55%が「より多くのビジネス上重要なシステムをBC/DR計画に組み込む必要性の増加」と回答し、48%が「拡大するIT統合により、BC/DRチームの管理対象となるべき潜在的な障害ポイントの増加」と回答している。

それでは不測の事態に見舞われた場合、その対策に掛かるコストについて考えてみたい。IBMが調査依頼し、ポネモン・インスティテュート社が実施した「2016年情報漏えいのコストに関する調査」によると1インシデント当たりの総コストはグローバルの383社平均では400万ドル、日本の27社平均では3億3,700万円という結果になった。これだけのコストが掛かるのでその予防策が求められるが、IT部門ではIT環境が複雑化する状況下で高度化するサイバー攻撃などを完全に防ぐことは難しいと認識している。情報漏えい発生原因については、「悪意のある攻撃」が48%、「システム障害」が27%、「人的ミス」が25%となっている。内的原因である「システム障害」と「人的ミス」が半数以上を占めているが、これらも事業継続対策の対象となるものである。

こうした問題への対策として事業継続マネジメント(Business Continuity Management:BCM)の重要性が注目されている。実際にBCM担当チームやBCMプログラムが関与することで情報漏えいの問題解決効率が向上し、発生時のコスト減少、回復時間の短縮をもたらしているという調査結果が出ている。「2016年情報漏えいのコストに関する調査」では、BCMの関与があったケースでは平均検出期間が52日短縮し、被害拡散防止時間は36日短縮できたとなっている。

ここまで情報漏えいに関して検証してきたが、事業継続で想定するリスクはほかにもさまざまなものがあり、グローバルで見ると地域によって重視するリスクや優先順位は異なってくる。日本で事業継続を議論する場合は自然災害が大半を占めるが、米国ではテロが対象の中心となる。だからといって日本でテロを想定しなくていいということではない。近年欧州でも頻発しているテロが日本を発生しないとは言い切れないのだ。このようにさまざまなリスクを想定して対策を講じることが重要になる。

BC/DR(レジリエンシー)に必要な視点 ―IBMが考える事業継続フレームワーク

さまざまなリスクに対応するためには、施設やITの対策だけでは不十分だといえる。そこでIBMでは実効性の高い対策を講じるためには「全体戦略」「ひと」「もの」の3つの視点から包括的に検討することが必要だと提言している。つまり、業務を俯瞰した影響範囲を把握して全体戦略を立案し、緊急時の円滑な情報共有と意思決定を促すために人的側面から体制を準備し、どのようなリスクにも耐えられる柔軟なITと施設を備えることによって十分なレジリエンシー対策が可能になる。

さらにこの3つの視点を詳細化し、レジリエンシーの検討において押さえるべき事項を7レイヤー・モデルとして提唱している(図1)。

この7レイヤー・モデルを災害発生から業務再開までの時系列な復旧計画に当てはめたものが図2になる。ここで重要となるポイントは「もの」に該当

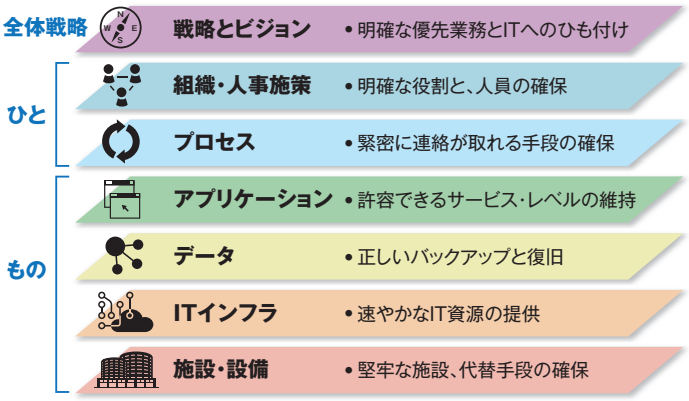

図1. IBMが考える7レイヤー・モデル

する「IT災害復旧計画(IT-DRP)による作業」の部分だ。多くの企業では全体戦略や人的な側面については何らかの対策を講じているが、「もの」については工場やオフィスなどに注意が向けられる。しかし、今の時代はITがなければ何もできないといっても過言ではなく、ITシステムやアプリケーション、設備などの復旧計画を準備することが重要なのだ。

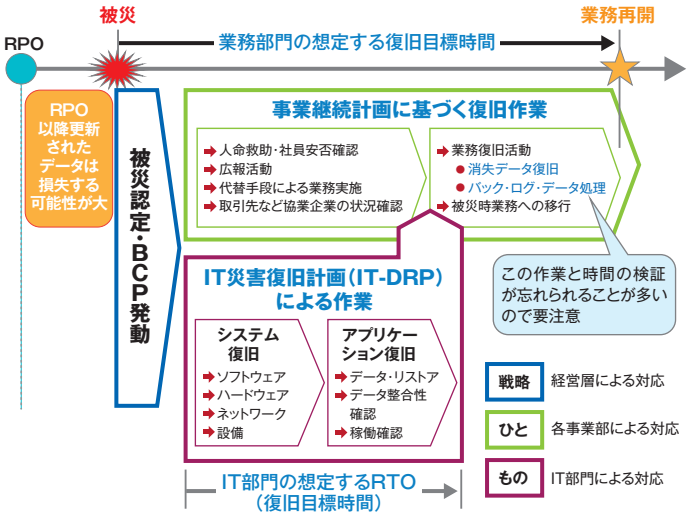

図2. 業務再開までの活動を支えるITの作業範囲

IBMでは、7レイヤー・モデルに合わせてさまざまなサービスを提供している(図3)。「戦略とビジョン」にかかわるコンサルティングから「施設・設備」にかかわるデータセンターの設計・施工といったものまで幅広い領域をカバーしている。またほかの企業とのアライアンスの下で提供するサービスも多い。The Weather Companyとのアライアンスで提供している気象情報に基づいた設計・構築計画などはその一例である。

特徴的なサービスとしては災対オフィスの提供が挙げられる。広域災害が発生した場合は地域全体が被災しているため、一時的な代替オフィスへのニーズは低い。しかし、テロなどによる局所的な被害の場合は災対オフィスへのニーズが高まる。特に外資系の企業の場合は、災対オフィスを事業継続計画に盛り込んでいるケースが多い。

これらのサービスから、幾つかのものを取り上げて以降で詳しく紹介する。

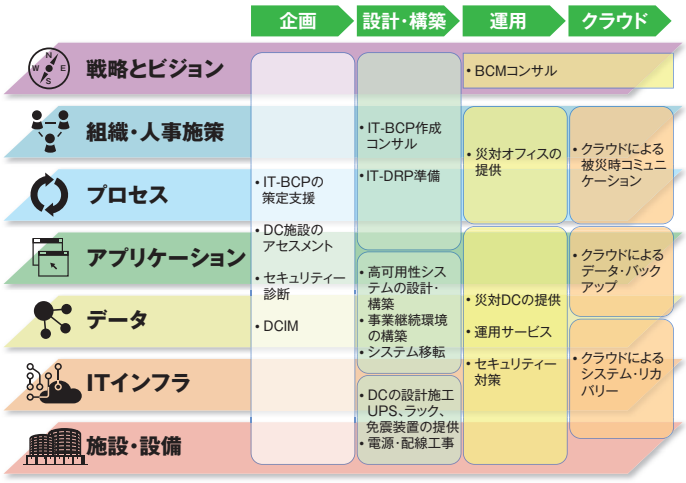

図3. 7レイヤー・モデルに合わせたサービス・ポートフォリオ

レジリエンシー・サービスの紹介 —コグニティブを活用したリスク分析の未来

IBMではコグニティブの技術によるIBM Watson Analyticsを活用したレジリエンシー・サービスを提供している。全世界で実施された事業継続に関する1,000件分の調査結果のデータがあるが、これをIBM Watson Analyticsに学習させることで「ナレッジ共有型の事業継続」を実現する。14の質問に対する回答をベースとして業界別、社員数別、地域別に事業継続の成熟度をベンチマークすることができる上、自由形式での質問に対する答えをレポートとして表示することも可能だ。このIBM Watson Analyticsの予知、予見、学習能力を活用することで事業継続を次のステップに推し進めることができるようになる。

レジリエンシー・サービスの紹介 —ハイブリッド・クラウド時代のレジリエンシー・サービス

ITシステムの災害対策は、以前はマシンを増やし二重化を図る対策が主流であったが、今ではコストや設置時間を削減するためにクラウドをバックアップに活用する考え方が普及している。IBMではクラウドを活用したレジリエンシー・サービスとして「クラウドによる被災時コミュニケーション」「クラウドによるデータ・バックアップ」「クラウドによるシステム・リカバリー」の3種類を用意している。

■ クラウドによる被災時コミュニケーション —IBM Resiliency Communication as a Service (RCaaS)

IBM Resiliency Communication as a Service（以下、RCaaS）は、災害時のコミュニケーションをサポートするツールで、e-メール、Twitter、各種センサーなどあらゆる情報を把握できることが大きな特長となっている。その情報に基づいて生成したイベントをリアルタイムに通知することができる。RCaaSは一般的なBCMの初動対応に活用することが可能だ（図4）。災害時に備えて策定された初動のワークフローをあらかじめRCaaSに登録しておくことで、災害時には収集された情報に基づいてRCaaSが次にとるべき行動を提示し、必要なメンバーにその内容を自動的に通知することができる。コミュニケーション・ツールといいながら、安否確認のための連絡や工場などに設置されたセンサーに異常がないかといった確認を自動的に行うなど、実作業の一部を受け持つ役割を果たす。ワークフローは固定的なものではなく、状況に応じて複数のパターンから柔軟に選択することが可能になる。

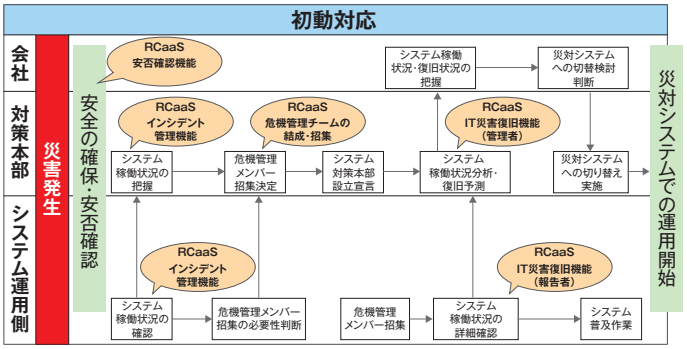

図4. RCaaSを活用したワークフロー定義の例

■ クラウドによるデータ・バックアップ —IBM Backup as a Service (BaaS)

IBM Backup as a Service（以下、BaaS）はクラウドを活用したデータ・バックアップ・サービスで、24時間365日のバックアップ管理を実現する（図5）。グローバルで300を超えるクラウド・レジリエンシー・センターが用意されているので、国をまたがったデータ保護戦略をサポートする。

BaaSの特長

- グローバルで同じレベルのサービス提供
- 従量課金
- 初期投資不要
- 成長に伴う拡張性と対応
- 要望の変更への柔軟な対応
- 高い信頼性とパフォーマンス
- 新しいサービス提供に伴うコスト削減
- 使用状況のレポート

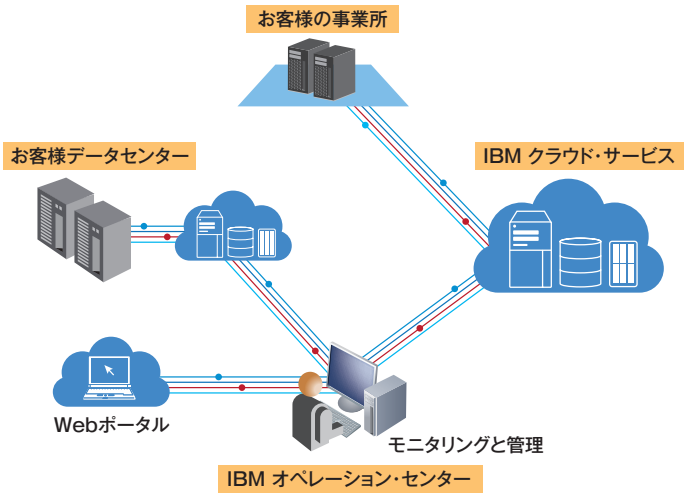

図5. BaaSの活用例

■ クラウドによるシステム・リカバリー —IBM Disaster Recovery as a Service (DRaaS)

IBM Disaster Recovery as a Service（以下、DRaaS）はクラウド・テクノロジーの活用で信頼性が高く、効率的なサーバー・リカバリーを提供。業務の速やかな再開をサポートすることが可能だ。

DRaaSの特長

・迅速なリカバリー：自動的なフェイルオーバーとフェイルバック
・RTOとRPOの短縮
・リカバリーの信頼性の向上
・物理サーバーと仮想サーバーで同様のサービスを提供
・Linux、Windows、AIXをサポート
・リモートからの自己管理ツール
・リハーサルや被災時の移動を回避

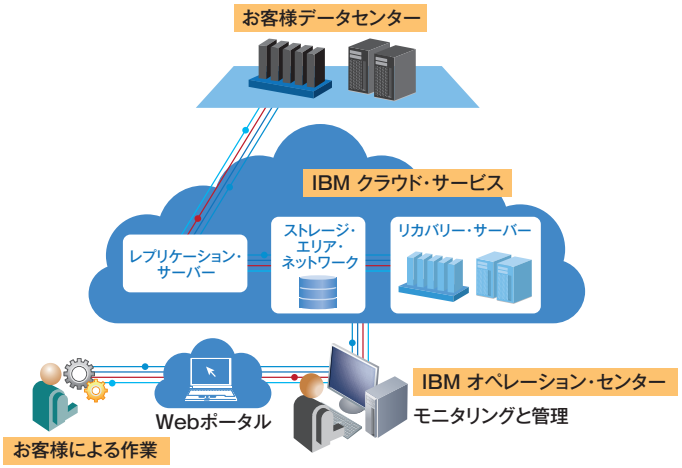

図6. DRaaSの活用例

“Always-on”の世界を目指して

IBMは50年におよぶ事業継続の実績をグローバルで積み重ねている。そして68カ国で400以上のデータセンターを有しているので、グローバルでビジネスを展開しているお客様の事業継続をサポートすることが可能だ。さらにIBMは世界最大のセキュリティー・サポート力を有している。従来のセキュリティーの考え方は、トラブル発生に備えるもので、基本的にマイナスをいかに減らすのかという点にフォーカスしていた。今は予報、予知に関するテクノロジーを活用することで、事前にいかに備えるかという考え方が中心になっているので、事業継続に適用することが可能だ。
またIBMはX-Forceというセキュリティー・オペレーション・センターを有しており、全世界のセキュリティー攻撃に関する情報を収集している。このX-Forceを活用することで高度なセキュリティー・サポート力を発揮することができる。
IBMはこうした事業継続に関するノウハウを活用して企業をサポートしているが、その際提唱しているのが“Always-on”という概念である。つまり事業継続は企業戦略として最も重要なものであるととらえ、全体を俯瞰した事業継続の戦略に最新のテクノロジーを活用することで常に災害や事故に備えることが重要だということだ。

IBMは長年蓄積したノウハウやテクノロジーを駆使することで、複雑化したIT環境における事業継続に関する課題解決を支援していく。

IBMレジリエンシー・サービスに関する詳細情報は
下記のWebサイトでご覧ください。
http://www.ibm.com/services/jp/ja/it-services/business-continuity/

IBMレジリエンシー・サービスのエキスパートが、分かりやすく解説した記事をブログに掲載しています。下記のブログをご覧ください。
ibm.biz/IBMResiliency_blog

日本アイ・ビー・エム株式会社
〒103-8510　東京都中央区日本橋箱崎町19-21

Printed in Japan
October 2016