時代遅れの災害復旧計画に潜む落とし穴を避けるために

ますます高まるビジネスへの期待および脅威に応じた新しい災害復旧アプローチが必要

IBM

目次

拡大する脅威の位置づけ

2012 年後半、ハリケーン・サンディがニューヨーク市一帯を襲い、ニューヨーク証券取引所は 2 日間閉鎖されました。ある意味、NYSE は幸運でした。その地域では、多くの企業が数週間も電力なしで過ごすことになり、1,800 便もの航空機がキャンセルされ、ニューヨーク市都市交通局 (New York City Transit Authority) は公共交通機関の運行を一時停止し、マンハッタン橋やトンネルは閉鎖されました。携帯電話基地局も 25% が被災し、事実上すべてのモバイル通信事業者のサービスが影響を受けました。

これまでに米国北東部を襲ったハリケーンの中で、サンディは最悪のものではありませんが、企業は現在テクノロジーに依存しており、そのテクノロジーには情報やアプリケーションの可用性を常時提供するものも含まれているため、多くの企業の災害復旧計画がサンディによって検証されたと言えます。人、テクノロジー、データ、スペースといった主要なリソースの可用性について、これまでになかった方法で考えるという課題が企業に突きつけられました。

フォレスター・リサーチによると、企業は現在、IT 予算のうち平均 6.2% を事業継続性および災害復旧に費やしています。これは、2010 年の費用の 1% 増に相当します。[1] しかし、これらのほとんどは自社運営の災害対策に費やされています。良好とはいえない経済状況やハードウェアのコスト削減を考えれば、かつては、自社運営の災害対策が当然の選択のように思えました。しかし、フォレスターが指摘するように、自社運営の災害対策は、技術や検査の不十分さに加え、全般的な関心の欠如など多くの問題に悩まされています。[2] このことは、ハリケーン・サンディの直後に、多くの災害復旧計画が適切に機能しなかったことで明らかになりました。多くの IT 幹部および企業経営者は、このハリケーンから得た教訓を踏まえて、自社の災害復旧戦略を再評価することにしました。

時代遅れの災害復旧計画にとってはまさに災難です。脅威は変化し、ますます拡大しています。ハリケーン、津波、竜巻、洪水、地震といった気象現象は、今やビジネスに対してより深刻な影響を与えます。テクノロジーに対する依存度がますます高くなっているため、障害が起こると致命的な事態になる恐れがあります。それに加えて、企業は世界の新興地域への投資 (特に IT 投資) を増やしています。この傾向から、組織は災害復旧の運用に一層焦点を当てる必要があります。新興国への投資は、複雑な災害対応をサポートするその国の能力をはるかに上回るからです。

また、中断や災害は、事業継続性以外の領域でも、組織に悪影響を及ぼしています。契約上の責任や売上損失のほかに、企業は今、データの可用性や復旧の基準の順守義務違反に直面しています。ソーシャル・メディアの時代においては、災害時の運用停止を含め、企業の不手際に関する情報はすぐに広がる恐れがあります。

中傷的なブログやツイート、投稿などは、組織の評判を損ないかねません。「2013 IBM グローバル・レピュテーショナル・リスクと IT に関する調査」[3] が示すように、自社のリスク管理の枠組みの中で風評被害に注目する組織の数が増えているのは、そのためです。

いざというときの災害復旧計画は適切に機能するでしょうか。それを判断するのは困難です。ほとんどの組織は、災害復旧を業務としていません。金融、製造、運輸といった業務に携わっています。度重なる災害時の運用から得られる経験もないまま、社内の事業継続性や災害復旧に携わるチームは、災害復旧戦略の開発、実装、テスト、維持において課題に直面する場合があります。整然とした環境にいながら、非常時のさまざまな事態を予測し、それに応じた計画を立てることは困難です。

いざというとき、現行の災害復旧計画は適切に機能しますか。それを判断するのは困難です。

しかし、IBM はお客様の災害復旧業務を支援しています。IBM は世界中の何千ものお客様の災害復旧をサポートしてきた経験から、多くの組織が災害復旧計画の基準として誤解しがちな点を 7 つ特定しました。

これらの基準はほんの 5 年～10 年前には妥当なものだったかもしれませんが、いまでは多くが有効ではなくなってしまったと IBM では考えています。データの増加、
IT 機能にアクセスするビジネス需要の増加、増大するデータセンターの占有スペースの管理、24 時間 365 日体制のアプリケーション可用性などに対応しなければならないなど、災害復旧への取り組みをより強化する必要が生じる一方で、IT 専門家が災害復旧について検討する時間がほとんどないという事態が生じています。本書では、これらについて詳しく解説するとともに、組織が災害復旧の取り組みを改革する際に役立つ IBM のサービスを紹介します。

災害復旧に関する誤解

IBM がこれまで災害復旧業務をサポートした経験から、非常に多くの組織が以下のような誤解をしていると考えます。

1 在宅勤務戦略をとっているため、災害時にも業務を継続できる。

災害後にできるだけ迅速に復旧するには、主要な従業員が業務を継続できるようにする必要があります。復旧計画の中には、在宅勤務の IT スタッフに依存するものもあります。

在宅勤務戦略は、多くの場合、当初の期待通りには機能しないものです。ビジネスに支障が出るような災害が発生すると、社員の自宅も同様に被災する場合もあるためです。避難が必要な社員もいるかもしれません。自宅にいる社員でも、オフィスで勤務するときと同じ情報やアプリケーションにアクセスできるとは限らず、生産性が制限されることもあります。

クラウド・ベースの災害復旧ソリューションは、どのような場所からでも業務の復旧を可能にする柔軟性を提供します。クラウドを Web ベースのポータルで管理することで可能になりますが、インフラストラクチャーだけでなく業務を復旧するには、資格のある IT スタッフと業務担当者が復旧現場にいることが重要です。災害時にはごくわずかな社員しか勤務できない可能性を予期し、災害復旧専門のスタッフを置くテクノロジー・プロバイダーとの契約を考慮する必要があるかもしれません。

2 **社員、お客様、サプライチェーンとの通信を可能にする、電話や e-メールをワイヤレスでやり取りする機能を備えている。**
社員、お客様、サプライチェーンのメンバーと連絡が取れなければ、また特定の状況ではメディアと通信できなければ、災害後に企業は業務を復旧できないかもしれません。そのため、災害時に通信を確保する計画を策定することが重要です。こうした計画では、企業の代表として話す権限が与えられている人物に関する指示、伝達する情報のタイプ、それを伝達する状況、時期、相手を決めておく必要があります。通信戦略は通信する相手によって異なります。例えば、災害時に主要な社員に伝達する情報のタイプは、メディアに伝える情報のタイプとは大きく異なるでしょう。社員が組織と連絡を取る必要性にも対応する必要があります。

通信計画を決めることと同様に、災害時の通信に使用するチャネルを決めることも重要です。一般的に、社内の通信には e-メールや電話が使用されます。より広範囲な通信には、印刷物、テレビ、ラジオが使用されます。しかし、多くの場合、災害時に一般の人々と情報をやり取りするソーシャル・メディア戦略には、さらなる改善が必要です。中には、ソーシャル・メディア戦略を全く考案していない組織もあります。IBM では、これは間違いであると考えています。組織が率先して Twitter、Facebook、LinkedIn、YouTube といったソーシャル・メディアで情報発信を行わない場合、部外者に内容を捏造される恐れもあります。

IBM は、災害時の通信としてソーシャル・メディア戦略を策定し、実施することを提案します。その中には、災害時のビジネス・レポート作成、コミュニティーのメンバーとの連携、懸念事項への対応が含まれます。

社員、お客様、サプライチェーンのメンバーと連絡が取れなければ、また特定の状況ではメディアと通信できなければ、災害後に企業は業務を復旧できないかもしれません。

3 **バックアップされたデータから、主要なビジネス・アプリケーションをリストアできる。**
2 次バックアップに磁気テープを選択することは適切です。ただ、リカバリー時間目標では 24 時間内の稼働を設定することも多く、磁気テープは 1 次バックアップとしては最適な選択肢とはいえなくなっているかもしれません。その上、磁気テープは場合によっては、不満を抱く何者かによって故意に破損される恐れがあります。さらに、磁気テープがひとつでも紛失したり損傷を受けたりするだけで、災害復旧作業全体が危うくなる恐れもあります。

また、磁気テープだけに依存すると、災害復旧現場に磁気テープを移送するという点でも課題に直面することになります。災害時には、道路は通行不能になり、地方だけでなく全国規模で交通システムが停止して、磁気テープを移送できなくなる場合

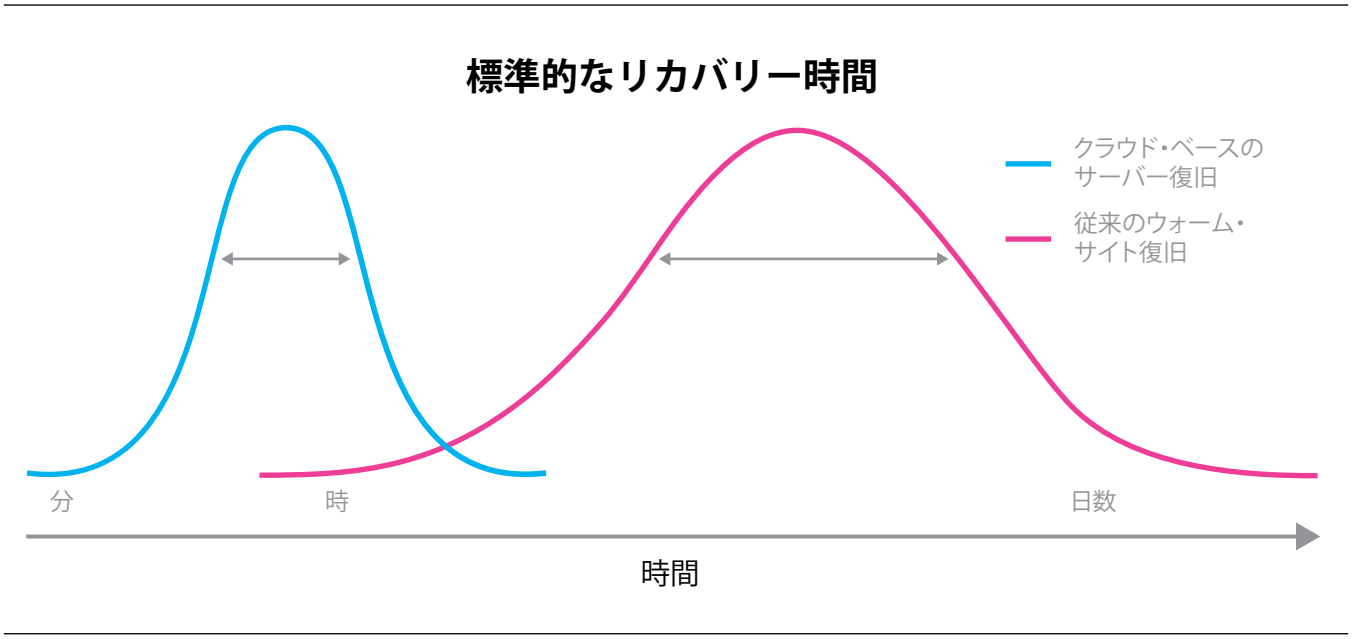

図 1. 従来の災害復旧アプローチを使用してアプリケーションを復旧する場合、一般には 33 時間から 50 時間かかることがほとんどです (左側の釣鐘曲線を参照してください) 。クラウド・ベースの災害復旧なら、復旧するサーバー台数にもよりますが、その時間を数分にまで短縮できる場合があります。

があります。そうした状況は、災害復旧計画に悪影響を及ぼします。少なくとも、輸送には予想以上の時間がかかり、リカバリー時間が許容範囲を超えることがあります。

たとえ、磁気テープを妥当な期間内に 2 次サイトに移送できたとしても、テープ・バックアップから運用をリストアするには相当の時間を要するでしょう。IBM の経験では、テープ・バックアップからの完全復旧には、最も順調に進んだとしても、一般的に約 20 時間を要し、最悪のケースでは約 80 時間を要することがあります (図 1 を参照してください) 。

24 時間体制のビジネスでは、最も重要なアプリケーションを数日ではなく数分または数時間で使用可能にする必要があります。そのような高可用性を実現する方法に、リカバリー時間目標が極めて短いクラウド・ベースの災害復旧サービスの採用があります。ただ、クラウド・コンピューティングにも制限事項やリスクはあるため、クラウド・テクノロジーを災害復旧計画に組み込む前には慎重な検討が必要です。

4

IT 作業の災害復旧計画を理解し、毎年テストを行っている。

リスクはますます変化しているにもかかわらず、多くの組織が何年も前に設定された災害復旧標準に固執しています。その典型的な例が、年 1 回の災害復旧テストです。この年 1 回のテストで災害復旧計画の有効性を証明できると、相変わらず多くの組織が信じています。しかし、この標準は、データセンター運用が非常に安定していた時代に設定されたものです。現在、アプリケーションは頻繁に変化しています。また、膨大なデータが絶えず生成され、多様なオペレーティング・システムが使用されます。さらに、インフラストラクチャーではしばしば物理リソースと仮想リソースが組み合わされています。1 カ月前にテストが正常に完了したからといって、現時点でのデータセンター運用の復旧が証明されるわけではありません。むしろ、一定間隔でしか実行されない災害復旧テストは、変更管理プロセスから災害復旧の取り組みを切り離してしまいます。さらに、一部のアプリケーションと IT 環境に限定してテストを行うことが非常に多いため、災害時に復旧計画がどのように機能するのかを判断する能力が一層制限されます。災害復旧計画が予想通りに機能するかどうかを判断するには、すべてのアプリケーションと環境で全面的にテストを行う必要があります。

そのうえ、災害復旧計画のテストではプロセス・スキルを考慮しない場合が極めて一般的です。災害時には、多くの IT リソースが直ちに使用可能になるとは限らないため、IT 運用には追加のプロセス・スキルが求められることがあります。したがって、IT リソースが再稼働するまで必要な手動タスクの実行に欠かせない「ハードウェア、ソフトウェア、アプリケーション」プロセスのスキルを持つ専門家を確保することが非常に重要です。クラウド・ベースの災害復旧サービスのプロバイダーを採用すれば、これが可能になります。そうしたプロバイダーは、簡単なテストの実施や、アプリケーションやデータのほぼシームレスな複製に対応できるからです。災害復旧の取り組みは、熟練した専門家に委ねられます。

5

2 次データセンター・サイトからデータセンターの運用を続行できる。

企業の構外にある 2 次データセンターから復旧操作を実行するのはよい選択です。しかし、非常に多くの場合、代替サイトは組織と近接しすぎており、災害の影響を逃れることができません。気象現象やテロ行為は、地域全体に影響を及ぼす可能性があります。たとえば、ハリケーン・サンディの場合、停電、公共交通機関の運行停止、通信の問題は、ニューヨーク市だけでなく、ロングアイランド、ニュージャージー州、コネティカット州の一部にも影響を与えたため、それらの地域の 2 次データセンターからの運用の復旧ができませんでした。反対に、組織の 1 次構内から離れた場所に 2 次サイトが置かれている場合、災害で航空機が不通になれば磁気テープやスタッフを 2 次サイトに移行できなくなる場合があります。

これらを克服するには、1 次サイトと 2 次サイト間のデータの複製および同期を実装する必要があります。そうすれば、バックアップ・メディアを移動させる必要がなくなります。こうした同期複製の試みにより、距離に関係するネットワーク待ち時間の問題が浮き彫りになります。「リアルタイム」のリカバリー・ポイント目標を実現するには、2 つのサイトを同期データ複製に対応できる近接距離に配置する必要があります。ただし、既に述べたとおり、サイト同士が近接しすぎる場合、組織の 1 次サイトが中断したときに、2次サイトも同じ影響を受けることがあります。反対に、2 次サイトが組織の 1 次サイトから離れすぎている場合、パフォーマンスは待ち時間の影響を受けるかもしれません。そのため、データ可用性に関する規制要件に従って運用している組織や、情報へのアクセス機能を失うわけにいかない組織は、データが非同期で複製される 3 次サイトの導入を考慮してもよいかもしれません。3 次サイトは、同じ破壊的な事象の影響を受けそうにない十分な距離を 1 次サイトおよび 2 次サイトとの間に保つ必要があります。

図 2. 組織の災害復旧計画では、社員の作業計画から、予想 IT 復旧時間に至るまで、あらゆることを誤解に基づき想定しているケースが多数あります。

2 つまたは 3 つのサイトの必要性を考えると、熟練した災害復旧プロバイダーとの契約が有効です。そのようなプロバイダーなら、2 次 (同期) または 3 次 (非同期) サイト、あるいはその両方を提供できるレジリエンシー・センターの大規模ネットワークを提供できるため、追加スペースの取得コストは発生しません。

テスト時のフェイルオーバーの成功で、事業継続性の能力が立証されている。
運用を復旧することと、業務を平常通りに戻すことは、全く別の問題です。運用を実動データセンターに戻すプロセスであるフェイルバックは、データセンターの通常運用を再開する最初のステップです。災害復旧フェイルオー

バー・モードで実行中に災害復旧サイトで作成されたデータは、フェイルバック・プロセス時に元の実動サイトに複製し直す必要があります。事業継続性および災害復旧計画でのフェイルバック手順はおろそかになりがちです。仮想化された復旧ソリューションの場合、一般的にフェイルバックは従来に比べて迅速で、それほど複雑ではありません。手操作による介入の必要が少ないことで、通常の運用に戻すために必要な時間および労力が大幅に削減されます。

7 **社員、通信、データ、アプリケーションの備えがあるため、災害から迅速に復旧できる。**

災害からの組織の復旧は、組織独自の復旧運用だけでなく、組織のサプライチェーンの構成要素の復旧操作にも依存しています。e-コマース業者は、災害復旧計画を改革し、それらを定期的にテストして、大災害の発生後でも迅速に運用を再開できるかもしれません。しかし、サプライヤーに商品を配送する手段がなければ、事業を完全には復旧できません。そのため、組織は自社独自の復旧操作だけでなく、サプライチェーンの上流から下流に至るまでの連携もテストする戦略を開発することが重要です。IBM は、重要なサプライチェーンの連携すべてに対するリスクを考慮し、適切な緩和対応を作成、文書化、テストすることを推奨します。

IBMがご支援できること

脅威の位置づけがますます拡大する中、多くの組織が現在の災害復旧計画の真のコストと機能に対する懸念を抱き、パートナーとの契約により最新の災害復旧運用を採用する価値を検討しています。実際、フォレスターによると、「Risks of 'Do It Yourself' Disaster Recovery」レポートで調査した組織の半数以上が、移行により災害復旧の総所有コストも削減できる場合には、災害復旧運用の一部または全体をアウトソーシングすることを検討すると報告しています。[4]

IBM では、災害復旧のアプローチはリスクの変化に合わせて進化させる必要があると考えます。企業は、災害復旧テストの頻度を増やしたり、非常時でも安全かつセキュアに通常業務を遂行できる環境を主要な社員に提供できるようにしたり、最も重要なデータやダウンタイムがほとんど許されないアプリケーションをクラウドに移行するなど、少しずつ対応を始めることができます。IBM は、これらの取り組みを支援する以下のようなサービスを提供しています。

- IBM Resiliency Consulting Services
- IBM インフラストラクチャー・リカバリー・サービス
- IBM 事業継続マネージメント・サービス
- IBM SmarterCloud Resilience Service

IBM Resiliency Consulting Services は、組織が復元力のある災害復旧策を成功裏に開発できるよう総合的なサービスを提供します。このサービスは、組織が復元力計画を設計、計画、実装し、インフラストラクチャーの復元力をテストするのを支援します。

IBM インフラストラクチャー・リカバリー・サービス は、ワークエリア・リカバリーと IT リカバリーの両方に対応します。IBM の **ワークエリア・リカバリー・サービス** により、組織は、中断時または災害時に 150 カ所のビジネス・レジリエンシー・センターで構成される IBM の世界中のネットワークで、代替作業環境を確保することができます。この安全性が極めて高いファシリティーは、パーソナル・コンピューター、電話、その他の作業ツールを装備したすぐに使えるワークステーションを提供します。

ファシリティーには、予備通信機能、マルチベンダーの IT 機器、無停電電源装置が装備され、IBM の復旧専門家が配属されています。また、モバイル IT 復旧オプションを利用できる地域もあり、一時使用のために選択しているサイトにモバイル・ユニットが提供されます。

災害復旧のアプローチは、リスクの変化に合わせて進化させる必要があります。企業は、災害復旧テストの頻度を増やしたり、最も重要なデータやダウンタイムがほとんど許されないアプリケーションをクラウドに移行するなど、少しずつ対応を始めることができます。

IBM の総合的な **IT リカバリー・サービス** は、ユーザーの固有のビジネス要件および技術要件に合うように調整できます。このサービスは、簡単なハードウェアの交換から、非常に複雑なミラーリングされた環境のプロビジョニングに至るまで、幅広く対応しています。ソリューションは、コンピューティング・ハードウェア、周辺装置、通信機器、オペレーティング・システム、インフラストラクチャーを含みます。総合的な復旧運用は、IBM の復旧サイトから実行できます。IBM 復旧サイトは、ワークエリア・リカバリーと同じ機能を提供します。

IBM 事業継続マネージメント・サービス は、障害発生時に重要なビジネス・プロセスの運用情報やビジネス情報へのアクセスを維持できるように支援します。これらのサービスは、統合された管理、モニター、データ保護、災害復旧をサポートします。IBM 事業継続マネージメント・サービスのポートフォリオから、組織はデータおよびプロセスの重要度に基づいて機能を選択できます。これらのサービスを全体的または部分的に管理および運用することにより、IBM は企業がダウンタイムを回避し、社員の生産性を向上させ、運用費を管理し、規制要件に準拠するよう支援できます。 **IBM マネージド・コンティニュイティー** は、1 次、2 次、3 次データセンターに、IT 対応の強固な専用データセンターのスペースと電力を提供し、IT インフラストラクチャーに高可用性のバックアップおよびリカバリー機能を提供します。データ・ルームの設計および実装と、進行中の管理サービスがすべて組み込まれています。

クラウド・コンピューティングは、災害復旧コンポーネントとしてますます利用されています。 **IBM SmarterCloud Resilience Service** は、災害復旧へのアプローチを改革する 2 つのクラウド・サービスを提供しています。それは、IBM SmarterCloud Managed Backup と IBM SmarterCloud Virtualized Server Recovery です。

IBM SmarterCloud Managed Backup は、パブリック、プライベート、ハイブリッドのクラウド・ベースで企業全体で情報の復元力とデータ・リカバリーを実現する、データ保護ソリューションを提供します。このサービスでは、自動化および標準化されたツールやプロセスを使用して、分散した情報を単一のインフラストラクチャーに統合することにより、バックアップを簡素化します。IBM SmarterCloud Managed Backup は、セキュリティー機能を強化した、非常に拡張性の高いソリューションです。このソリューションを使用して、バックアップの優先順位、データ保持・検索の目標、データ保護と拡張性のニーズに応じて計画、実装できます。これにより、バックアップ・エラーや、手操作による介入の必要を削減できます。また、磁気テープとクラウドを用いたハイブリッド手法でのデータ・バックアップには、テープ保護および管理サービスが提供されています。

IBM SmarterCloud Managed Backup がデータ復旧サービスであるのに対し、**IBM SmarterCloud Virtualized Server Recovery** は、サーバーおよびアプリケーション復旧サービスです。IBM SmarterCloud Virtualized Server Recovery は、速さ、信頼性、コストの面でより優れた IT インフラストラクチャーの復旧を実現するクラウド・サービスです。このサービスは、ほぼ即時に復旧を実現する高度なフェイルオーバー/フェイルバック機能を提供します。さらに、物理サーバーと仮想サーバーを混合したサーバー環境を復旧する機能も備えています。サービス・レベルが階層化されているため、アプリケーションの重要性およびダウンタイムの許容度に基づいて、アプリケーションに優先順位を付けて管理できます。また、IBM SmarterCloud Virtualized Server Recovery を既存のインフラストラクチャー・リカバリー・サービスと統合して、総合的で全体的なホットサイト・ソリューションを実現できます。

始めるにあたって

時代遅れの災害復旧戦略を改革することは、非常に困難です。まず、以下の点を考慮してください。

- 有効な災害復旧プログラムの実行と保守に年中無休で対応可能な、専門知識を持つ人材が社内にいますか。
- 災害復旧プログラムに継続的に資金を投入できますか。
- 一貫性があり、頻繁に実施されるテスト計画や訓練計画がありますか。
- 万一被災した場合、バックアップ・データやシステムに迅速かつ有効にアクセスできますか。
- 現在の事業継続性ソリューションは、変化する要件に対処できるほど拡張性が高いものですか。
- 1 日分、1 週間分、1 カ月分の重要なデータを失った場合、業務にどのような影響がありますか。
- 長期間、重要なアプリケーションを利用できない状況に置かれた場合、業務にどのような影響がありますか。

組織は、災害復旧計画の改革を始めるにあたり、これらの考慮事項を念頭に置く必要があります。その上で専門的な知識が必要であると判断した場合、IBM Resiliency Consulting Services がきっとお役に立てると考えています。クラウド・コンピューティングを使用してデータとアプリケーションの保護を強化する場合、IBM はクラウド移行への正しいアプローチを提供します。このアプローチでは、ビジネス復元力を実現するエンドツーエンドのクラウド戦略を考案し、クラウド移行の計画を立案し、マイグレーション、標準化、登録など移行そのものを行います。

まとめ

災害復旧はかつてないほど重要になっていますが、非常に多くの場合、関心の欠如、資金不足、不十分なスキルによって対策が進んでいません。それに加え、経験不足から災害対策に関する知識を蓄積できていないため、自社の戦略ではさまざまな事態を予想できず、不適切な対応となりかねません。IBM は、ビジネス復元力および情報保護において 50 年以上の経験を有しているため、お客様に適切なご支援を提供することが可能です。IBM には、さまざまなリカバリー・ポイント目標およびリカバリー時間目標に対応する、幅広いサービス・ポートフォリオがあります (図 3 を参照してください)。50 カ国に 150 カ所のレジリエンシー・センターを設置し、1,800 名以上の災害対策専門家を配属しています。

IBM は、クラウド・ベースのデータ・バックアップおよびサーバー・リカバリーの領域でリーダー的存在として広く認められており、重要なデータおよびアプリケーションを保護し、それらを数分でリストアする機能を提供しています。IBM のサービスなら、お客様の災害復旧ニーズに応じてソリューションを構成できます。さらに、社員の生産性をサポートし、収益や評判の損失を回避可能にするため、総所有コストが自社で策定した計画に比べ抑えられるケースがほとんどです。IBM はこれらのサービスで、時代遅れの災害復旧に潜む落とし穴を回避できるようご支援いたします。

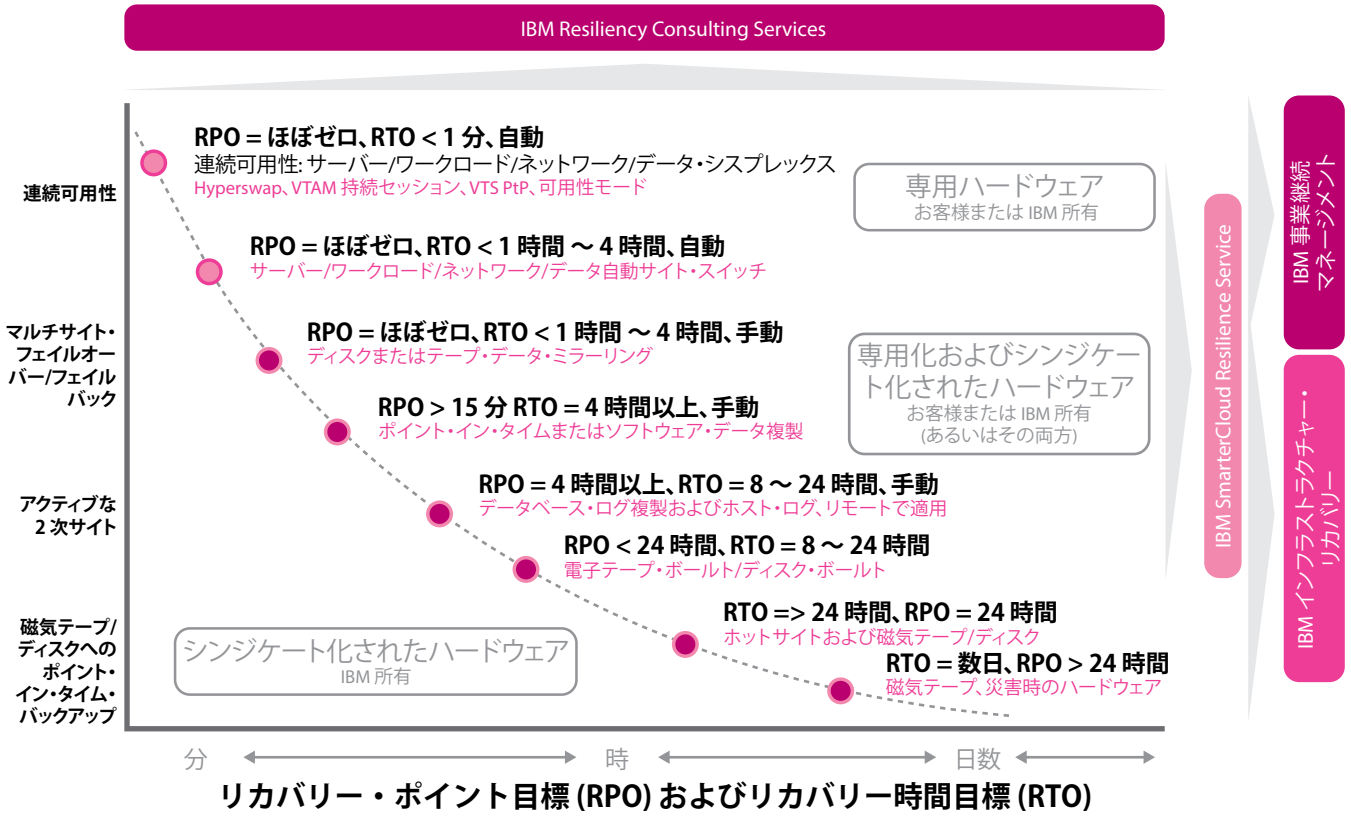

図 3. IBM Resiliency Consulting Services は、さまざまなリカバリー時間目標およびリカバリー・ポイント目標をサポートするさまざまなアプローチを提供します。ビジネス上最も重要なアプリケーションでは連続可用性アプローチを選択し、それほど重要とはみなされないアプリケーションでは復旧時間を長くとることも可能です。

詳細情報

IBM 災害復旧サービスの詳細については、IBM の営業担当員またはビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。

ibm.com/services/jp/ja/it-services/bcrs.html

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

IBM のホームページは以下をご覧ください
ibm.com/jp/

[1, 2, 4] *The Risks of "Do It Yourself" Disaster Recovery*、2013 年 1 月に、IBM の委託によりフォレスター・コンサルティングが実施した委託調査。

[3] *Six keys to effective reputational and IT risk management (風評と IT に関するリスクを効果的に管理するための 6 つのポイント)*、IBM、2013 年。

Please Recycle

BUW03031-JPJA-01