JIG-SAW

ITシステムのBCP対策で
知っておきたい6つのポイント

JIG-SAW株式会社

電話 03-6262-5160

サービス問合せ https://ops.jig-saw.com/form/contact

Webサイト https://ops.jig-saw.com

システム運用代行
に関するお問合せはこちら

　※本資料は2021年5月に作成されたものです。掲載されている各種情報は作成時点のものです。

はじめに

BCP(事業継続計画)とは、企業が自然災害やITシステム障害などが発生した際に、事業をできる限り中断させないようにあらかじめ方針や手順、体制などを定めておくことです。

内閣府が行った平成29年度の「企業の事業継続及び防災の取組に関する実態調査」(*1)によると、大企業では6割強、中堅企業では3割強がBCPを策定しており、さらに策定中を含めると大企業では8割強、中堅企業では5割弱となり、年々各企業の取り組み意識が高まっています。日本では地震や水害などの自然災害も多く、また新型コロナウイルス感染症のような不測の事態も起こりうる現代において、事業停止のリスクに備えておくことはきわめて重要です。

また現在の事業活動においてはITシステムに頼るところが大きく、これらを構成するサーバーやネットワークの障害も事業継続性に影響を及ぼすため、対策が不可欠です。

本コンテンツでは、ITシステムのBCP対策について焦点をあてて説明します。

ITシステムが引き起こす事業停止のリスクとは？

事業活動のITシステムへの依存

冒頭でも述べたように現在の事業活動においてはITシステムに大きく依存しており、システム障害が起きると事業の中断や停止に直結します。とりわけITサービスを事業の中核に置いている企業にとっては顧客離れや経営悪化などにも繋がる恐れがあります。

外部ITサービスへの依存

ITシステムを稼働させるには自社だけで完結できることは稀であり、電力やインターネット回線をはじめとして、近年ではクラウドインフラやSaaSの利用など外部から提供されるサービスに依存する割合が高くなっています。

このため、自社のみがしっかりBCP対策を行ったとしても、これら外部提供のITサービスの事業継続性も把握しておかなければ、事業の中断が長引いたり、早期復旧に支障が出たりといった問題が発生するリスクが高まります。

平時にも起こりうるシステム障害

システム障害は災害時のみならず、平時においても発生する可能性がありますので注意が必要です。

ITシステムのBCP対策を検討するにあたっては、「システム障害による事業の中断や停止を回避すること」、「事業の中断や停止が発生した際はできるだけ速やかに復旧させること」の２つの面を考慮する必要があります。

*1 「平成30年6月 企業の事業継続及び防災に関する実態調査結果の公表について」より引用

ITシステムのBCP対策の進め方

BCP対策を進めるにあたって抑えるべき6つのポイントについて説明します。計画を立てるには、以下のステップで行うとよいです。(図1)

ポイント1
復旧目標値の決定

どこまで対策を行うかといった決まりはないため、はじめにシステムの重要度や予算等に応じて障害が発生した際の復旧目標値を定めます。これには次の指標があります。

・【目標復旧レベル】
RLO（Recovery Level Objective）
どの程度の業務範囲や稼働状況まで復旧させるかを定めます。

・【目標復旧時間】
RTO（Recovery Time Objective）
目標復旧レベルまでどの程度の時間で復旧させるかを定めます。

・【目標復旧時点】
RPO（Recovery Point Objective）
どの時点までのデータを復旧させるかを定めます。

ポイント2
ITインフラ及びサービスの選定

自社で定めた復旧目標を達成できるようにITインフラやサービスを選定します。この時考慮すべき事項は次のようなものが挙げられます。

・オンプレ環境にシステムを構築する場合は収容先のデータセンターの立地や非常設備を確認する。

•クラウド環境にシステムを構築する場合はリージョンやゾーン/アベイラビリティゾーンが充実したベンダーを選定する。

•SaaSを利用する場合はサービスレベルを確認する。

•テクニカルサポートや運用委託など人に依存するサービスを利用する場合は緊急事態発生時の体制やどの程度までサービスを受けることが可能か確認する。
- 緊急連絡先の有無
- 通常時と災害時のオペレーターの対応品質
- サービス提供事業者の拠点の場所や立地

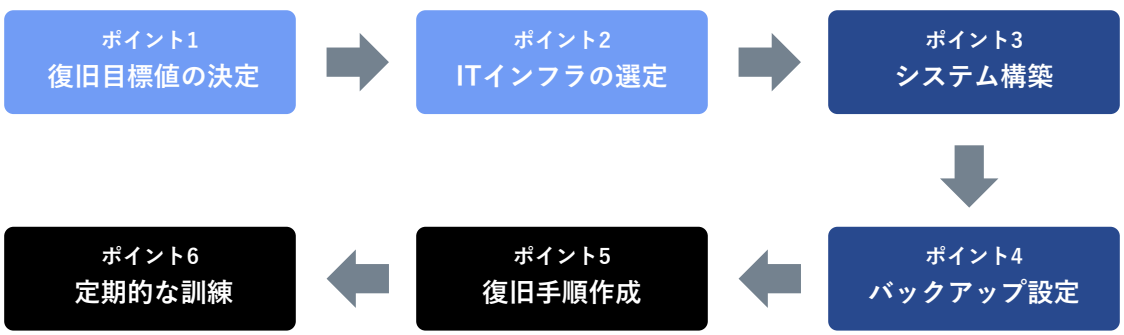

図1 BCP対策の進め方

ポイント3
障害に強いシステムの構築

障害に強いシステムを構築するには、オンプレやクラウドに限らず単一障害点をできる限り無くす事が基本となりますので、冗長構成で構築することが望ましいです。冗長構成はできるだけ遠隔地に配置をするのが望ましいです。オンプレミスの場合は、遠隔地に複数の拠点を設けるのは難しい場合があるかもしれませんが、クラウドを利用する場合には冗長化されたデータセンター(AWS/ Azureの場合：アベイラビリティゾーン、Google Cloudの場合：ゾーンと呼ぶ)やリージョンに配置することを検討します。

自然災害が発生した直後は、電話が繋がりにくく連絡が取りづらい状況となったり、交通機関の停止により通勤が困難となったり、停電により通信経路の確保が困難になるなどの恐れがあり、この間はシステム障害が発生しても十分な対処ができない事が予想されます。クラウドを利用している場合は、マネージドサービスの利用を検討します。また、システムを監視するツールやサービスの中には、アラートをトリガーにしてあらかじめ設定しておいたコマンドを自動的に実行することができる機能を持つものがありますので、これらを活用できないか検討することも一つの手です。

ポイント4
データバックアップの設定

自社で定めたRPOを満たすようにデータの定期的なバックアップを行います。バックアップデータ自体を保護するために、多重化や別媒体の保管を検討します。クラウドストレージのサービスを利用する場合、ストレージの種類によっては取り出す際に時間を要するものもあります。SLAや仕様を十分に確認のうえ選定することが望ましいです。

またバックアップが正常に取られているかをきちんと確認する必要がありますので、バックアップ成否の監視や通知なども設定します。

ポイント5
復旧手順の作成

最後に復旧までの作業手順を作成します。
障害が発生した際の通知～復旧のフローも整えることで、緊急時に落ち着いて対応することができ、復旧時間の短縮にも繋がります。

ポイント6
定期的な訓練

作成した復旧手順にしたがって定期的な訓練を行い、問題点や改善点がないか、各復旧目標値の達成に無理がないか等を点検することが重要です。

おわりに

本資料ではITシステムのBCP対策について焦点をあててご説明しました。BCP対策は必ずこれを行わなければならないという決まりはないため、自社の方針や目標を明確にすることが大事です。

また、BCPは一度策定すれば終わりではなく、継続的に見直しや改善を行うことが必要不可欠です。初めから完璧なものを目指すと、いつまでも策定が終わらず計画倒れとなったり、世の中の状況が変化し対策の有効性が失われたりする可能性もあります。これらの理由からも、運用しながら改善サイクルを回すことが重要です。

あなたのシステムにひとつ上のサポートを

JIG-SAWは、これまでにないシステム管理・支援サービスを提供します。
クラウドをはじめとしたあらゆるシステムの「サポート」を科学し、企業の成長を後押しします。

あらゆるシステム管理とサポートを強化

「JIG-SAW OPS」

クラウドや自社で保有されているシステム環境を、管理者様に代わって24時間体制で管理し、企業のシステム管理体制を強化します。
JIG-SAWが開発した「puzzle」を使用した異常検知/自動通知の仕組みと、エンジニアによる技術サポートを組み合わせたサービスをご提供します。お客様が本来の業務に注力し、事業を最大化できるよう、システム管理の側面から全面的にサービスを支援します。

ひとつ上のマルチクラウド包括支援サービス

「JIG-SAW プライム」

Amazon Web Services、Google Cloud、Microsoft Azureを、高いコストパフォーマンスでご利用いただける、マルチクラウドの包括支援サービスです。企業やプロジェクト単位で複数のクラウド、複数のアカウントをお持ちの場合でも、円建ての請求書発行から問合せ窓口まで、一元的に支援します。お困りごとがあれば、クラウドエンジニアによるプロフェッショナルで高品質なサポートをご利用いただけます。

JIG-SAW

お問い合わせ
TEL 03-6262-5160

JIG-SAW株式会社　〒104-0028 東京都中央区八重洲2丁目2-1　東京ミッドタウン八重洲 八重洲セントラルタワー33階
WEB：https://ops.jig-saw.com