災害やサイバー攻撃から従業員とその業務をどう守るか

BCPとBCM策定・見直しのポイントを理解する

日本は昔から自然災害の多い国と言われてきました。特に近年、地震や台風、噴火、豪雪、洪水など、過去にない異常気象や大災害に見舞われることが増えています。また、インフルエンザなどの感染症の爆発的な流行も私たちのビジネスや日常生活に多大な影響を与えてしまいます。最近では、サイバー攻撃やテロ、情報漏えい事件と、それに伴うシステム停止など、トラブルへの対策も必須です。私たちの暮らしにICTが密接に関わるようになったことで、災害によるシステムトラブルへの備え、BCP対策の重要性が高まっています。

システムを早期復旧するためのBCP対策の重要性

ひとたび大規模な災害などが発生すると、ビジネスへの影響範囲は計り知れません。例えば、「交通網が止まってしまい、従業員が出社できない」「システムダウンなどで日常業務が行えない」「従業員の安否確認が取れない」「取引先への連絡が取れない」という状況が出てきたりします。

自社だけが影響を受ける災害の場合は、取引先に迷惑をかけることにもなり、場合によっては違約金、契約違反などに発展するケースも出てくることもあります。また、取引先や利用中のクラウドサービス・ネットワークなどが被災した場合、自社ビジネスにも影響するケースが起こりえます。例えば、製造業の場合、取引先から入ってくるべき原材料や部材が急停止することで、自社の生産が停止してしまうということも過去には起こっています。

そうした中、多くの企業で、被災後に速やかに普及したり、非常時でも事業を継続する仕組みを構築したりすることが強く求められるようになりました。「BCP（事業継続計画）」や「BCM（事業継続マネジメント）」、「BCMS（事業継続マネジメントシステム）」とも呼ばれています。

BCP／BCM策定のポイントとは？

BCPの重要性が強く認識されたのは、2011年の東日本大震災がきっかけだと言われています。災害対策の重要性は以前から指摘されていて、実際にBCPを策定していた企業は存在していました。しかし、実際に被災した企業を対象にした調査では、「十分に機能した」と回答した企業は1割程度だったとのことです（日本情報システム・ユーザ協会「JUAS」調べ）。

BCPやBCMを策定することで、被災時に素早く対処し、事業を継続できるようになります。ビジネスとICTが密接に結びついた現在、BCPやBCMは情報システム部門（以下、情シス部門）にとっても非常に重要です。

今では、企業規模や業種を問わず、あらゆる企業での対策が求められるBCP。その策定ポイントとは何でしょうか？　以下で考えていきましょう。

災害やサイバー攻撃から従業員とその業務をどう守るか

問題が発生した場合は、「現状把握」→「一時的な対処」→「復旧」という流れが基本的な対策となります。この流れ自体は一般的なトラブル発生時と変わりません。

まずは、どのような被害があるのか「現状」を把握することです。現状を理解することで、事業を継続するのに何が不足しているかを踏まえたうえで次に取るべきアクションが分かります。迅速に情報がエスカレーションされる組織作り、被害情報が適切な部署に過不足なく届く仕組みも、現状を把握するのには重要です。

次に、事業を素早く継続するために必要な対処を行います。担当者以外が業務を引き継げる状態にしたり、不足している設備やネットワークを「代替・移行」する仕組みを整えたりします。事前に業務に必要な資材や設備を把握し、その代替手段を取りまとめて、出来ることや出来ないことも明確にしておくことが重要です。

最後に、災害によって被害を受けた部分を「復旧」していく仕組みを整えます。会社施設や設備といった物理的な復旧、ネットワークやシステムなどの技術的な復旧をすることで、徐々に本来の業務へと戻していけるようにしていきます。この際に、一気に復旧すると業務が集中し二次災害が発生する事もあり得るので注意が必要です。

BCP／BCM 策定の基本的な考え方

現状把握	一時的な対処	復旧
どのような 被害があるのか	事業を素早く継続する ために必要な対処	物理的・技術的な復旧

「現状把握」→「一時的な対処」→「復旧」という流れが基本的な対策となる

こうした被災の影響を最小限に抑えるためには、事業を早期に回復させるためのマニュアルをあらかじめ作っておくことが必要です。そこで重要になってくる考え方が、BCPなのです。

BCPを対象とする業務については、収益の多くを占める「中核事業に絞る」ことがポイントです。全てを完璧に対応するコストを考えると、手当たり次第に対応するのではなく、ビジネスや社会への影響度などを検討したうえで、リスクの大きいもの、経営的に重要なものから対処していくことが求められます。

情シス部門が取るべきBCP対策

次に、情シス部門が取るべきBCP対策について考えてみましょう。

●ICTインフラ対策

近年、自社内でシステムを保有するオンプレミスから、外部のデータセンターやクラウドサービスなどの利用が主流になりました。
多くのデータセンターでは「停電対策」として無停電電源装置や自家発電設備を備えています。東日本大震災後の計画停電時に一部が実際に稼働したとも言われている、こうした仕組みを持つデータセンターにシステムが入居していれば、無停止で事業を継続することも十分可能になります。

しかし、災害時などでサーバーを運用するデータセンターが堅牢でも、そこに至るネットワークに障害が発生し、システムを利用できないといった状況も考えられます。

このようなICT環境における災害対策の一環として考えられるのが、「ネットワークの冗長化」です。例えば、拠点間、あるいは拠点とデータセンターを接続するネットワークにおいて激甚耐性をもつ冗長化がされていれば、一方が切断されてもバックアップ回線で通信を継続できる環境を整えられます。ネットワークの冗長化をセットで導入できるデータセンターを選ぶことも可能です。

●ICTシステムの早期復旧対策

ICTシステムやデータなどが企業の経営基盤の中で重要な位置を占めるようになっています。必然的にシステムやデータの損失を防ぐためのリスクマネジメント施策であるバックアップは、経営課題であるBCPにおいても重要事項に位置づけられるようになりました。
ICTシステムの冗長化としては、機器自体を複数台準備し、運用系が故障すると待機系に切り替えるなどの運用方法もあります。BCP対策においては、アプリケーションやデータベースといったサーバーシステムのバックアップや冗長化などの対策は必要不可欠となっています。昔はシステムのバックアップと言えば、システム単位にデータをテープ媒体に保存することでした。しかし現在は、早期復旧を目的とするためのコストに応じたリカバリー対策が進んでいます。具体的には、「DR（ディザスタリカバリー）」サイトでの最低限の業務継続やセカンダリサイトの構築、遠隔地におけるバックアップなどが挙げられます。

特に、遠隔地バックアップは、今後発生が想定される首都直下型地震や南海トラフ地震など災害時に特定地域が被災する場合を考慮した際、企業が保有する大事なデータを国内でも遠く離れた別のデータセンターで確実に保護するための重要施策となってくると考えられます。

BCP対策では、単にシステムやデータのバックアップを取るだけでは不十分です。事業を継続して早期復旧を図るためには、リアルタイムのバックアップ／リストアという手順、あるいは完全同期された遠隔地データセンターへの即座のクラスタリングなどが実現できるソリューションも求められます。データセンターやクラウドサービスを選定する際は、クラスタリングの実績の有無や、自社システムでの長時間のバッチ処理やトランザクション障害など実際の運用も含め、バックアップサービスについても併せて検討していくことが重要です。

●非常時の社員との確実な安否確認

緊急時に従業員の安否確認や取引先の被災状況を素早く把握することも非常に重要です。災害発生時には、設備の破損や電力不足、通信量の急増に対する通話規制などが起こります、そのため、固定電話や携帯電話での安否確認や緊急連絡が困難になることも予想されます。

過去の大規模な震災では、IP電話や電子メール、SNS（Social Networking Service／Social Networking Site）といったインターネットを使った通信手段が役立つ場面が多数見られました。そうした通信手段の確保もBCP対策では非常に重要となります。ただ、被災の規模や範囲によっては、必ずインターネットが使えるとは限りません。企業のBCP対策としては、複数の連絡手段を準備したり、一時的な通信回復時でも利用可能な情報集約体制を整えておくことが必要です。

●遠隔作業を可能にする環境の整備

事業を継続するためには、万が一、出社できない状態になっても従業員が業務を継続できるような体制を取ることも重要です。自宅や社外からICTシステムへアクセスできる環境を整備することも求められます。具体的には、仮想デスクトップやVPNなどで、セキュリティー上も安全に社外からアクセスできるデバイスや通信回線を準備することが挙げられます。

これらのツールを活用することで、ネットワーク環境さえ利用できれば、企業システムにアクセスして業務やサービスを継続可能になります。インフルエンザやはしかの流行などへの対策としても注目されています。

●サイバー攻撃発生時も考慮する事業継続対策

IoTの普及に伴い、業務やサービスに関わる機器の多くが常にインターネット上に接続され、サイバー攻撃をはじめとした様々な攻撃に実際にさらされています。ビジネスへのインパクトを考えると、大規模な自然災害を想定した現状のBCPに加え、サイバー攻撃によって発生するリスクも想定したBCPを併せて策定しておく必要があります。社内だけでなく社外のセキュリティー有識者との体制構築も場合によっては必要となります。

徹底した防衛措置を行うとともに、万が一の被災を想定した事業継続計画を立案して、具現化するとともに、特にデータ流出やシステムダウンなど最新のサイバー攻撃を見据えて継続して見直していく取り組みが求められます。

災害やサイバー攻撃から従業員とその業務をどう守るか

情シス部門が取るべきBCP対策

ICTインフラ対策

・拠点とデータセンターを接続するネットワークにおいて激甚耐性をもつ冗長化
・データセンターでは「停電対策」として無停電電源装置や自家発電設備の設置

完全同期された遠隔地データセンターへの即座のクラスタリング

・DR（ディザスタリカバリー）サイトでの最低限の業務継続やセカンダリサイトの構築
・完全同期された遠隔地データセンターへの即座のクラスタリング

非常時の社員との確実な安否確認

・複数の連絡手段を準備し、情報集約体制を整える

遠隔作業を可能にする環境の整備

・仮想デスクトップやVPNなどで、安全に社外からアクセスできるデバイスや通信回線を準備

サイバー攻撃発生時も考慮する事業継続対策

・最新のサイバー攻撃を見据えて継続して見直していく取り組みが重要

情シス部門が取るべきBCP対策のポイント

普段使っているICTツールの見直しもBCP対策に有効

BCPは万が一の事態に備えて策定しますが、策定したBCPを陳腐化させずにより実効性を高くするためには、計画の策定から定期的な運用、評価、計画の見直しといったBCMを実践することも重要です。BCMによる継続的な維持・改善に取り組み、被災による損失を最小限に抑え、迅速に事業再開することが新たな機会の創出にもつながります。業務の優先順位付けや影響分析は、定期的に見直すことが大切です。

事業継続にICTが欠かせない存在となった今、その運用管理を行う情シス部門の責任も重大となってきました。しかし、非常時用システムを特別に用意したとしても、いざというときになって初めて使うようでは、「使い方が分からない」といった問い合わせが情シス部門に殺到し、冒頭のように「十分に機能しない」ことになりかねません。

普段から使っているツールを、なるべく非常時にも使えるようにしておくこともBCP対策の基本の1つだと言えます。そのためにも、ICTツールの見直しや検討も重要な業務となっています。ICTツールに関しては、働き方改革など普段からのテレワークが推進されています。BCPの観点についても併せて検討してみてはいかがでしょうか。

【 制作／コンテンツブレイン 】

NTTコムウェア株式会社
URL：https://www.nttcom.co.jp/

WEB 掲載：2019.3