やさしい「ITサービス継続」

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp

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

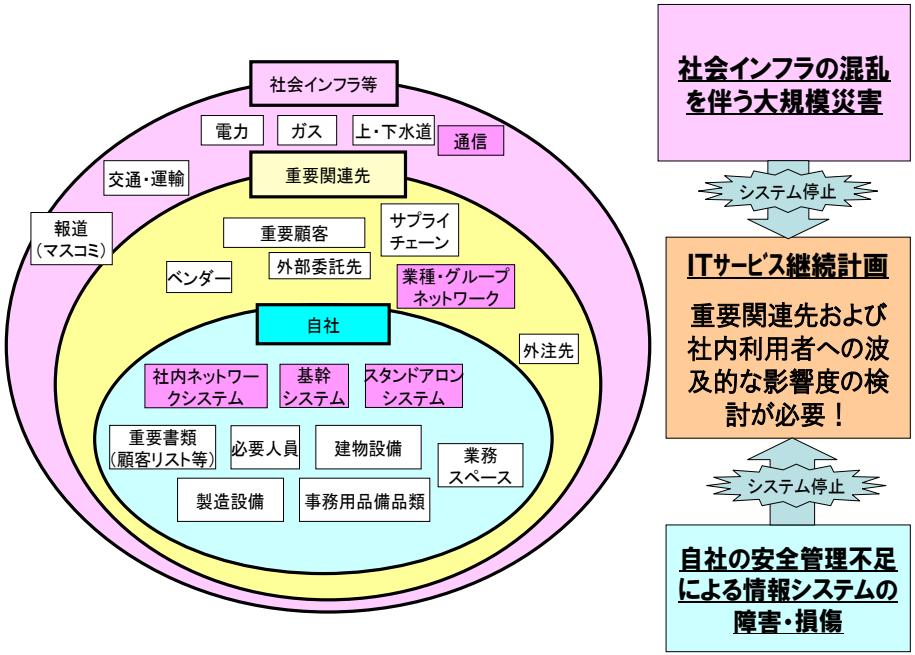
はじめに

アメリカで発生した９．１１テロは莫大な被害と犠牲を社会に与えたことは、まだ大きな印象を記憶に残しています。この被害の中で、ある保険会社は業務継続のためのあらゆる手段を、各ベンダーとも協力して講じ、わずか数日で基本的な業務を再開するという離れ業を成し遂げました。企業にとって、不測の事態が発生したとき、如何に短期間で業務を再開できるかは、存続にかかわる大きな要素です。日頃から、不測の事態への対応を考え、対策しているか否かは、既に業務推進のコアとなりつつあるＩＴシステムについて特に重要な項目となります。

この機会にＩＴサービス継続について一考して頂き、本冊子が事業の継続対策について、その検討の一助になれば幸いです。

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

情報システムを取り巻く社会環境とITサービス継続計画



出典：経済産業省　「ITサービス継続ガイドライン」

１．ＩＴサービス継続とは

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います。

ＩＴシステムが長期間停止することで、取引先からの受注状況がわからなくなったり、社内の連携が取れなくなったりするなど、企業活動に重大な影響を与えることも危惧されています。

平時に発生したシステムトラブルからの復旧時間を短縮することはもちろんですが、自然災害や事故などが発生したときでも、いかに短期間でＩＴシステムを復旧し、企業活動を再開するかが、取引先や顧客との信頼関係に影響します。

※ＩＴサービス：組織における業務の遂行に際して必要となるＩＴ及びＩＴに関連する体制の組み合わせによって提供される機能。

（経済産業省　「ＩＴサービス継続ガイドライン」より）

企業活動になくてはならないIT

対象とするシステムの数・種類や目標とする復旧時間の長さにより、必要となるコストが変わってきますので、どのシステムの復旧を優先するか、復旧をいつまでに行わなければならないかといったことを検討する必要があります。

例えば、ＩＴシステムが停止した場合でも、手作業で対応可能である業務ならば、そのＩＴシステムの復旧の優先度を低くすることができます。

逆に、取引先や顧客からの連絡を電子メールのみで受けているような場合は、電子メールシステムの復旧の優先度を高くする必要があるかもしれません。

このように、災害、事故等の発生に際し、ＩＴサービスの中断・停止による事業継続に与える影響を、求められるサービスレベルと対策に必要なコストとの関係の中で最適化するための取り組みをＩＴサービス継続といいます。

手作業で対応

電子メールで受付

事業継続検討会

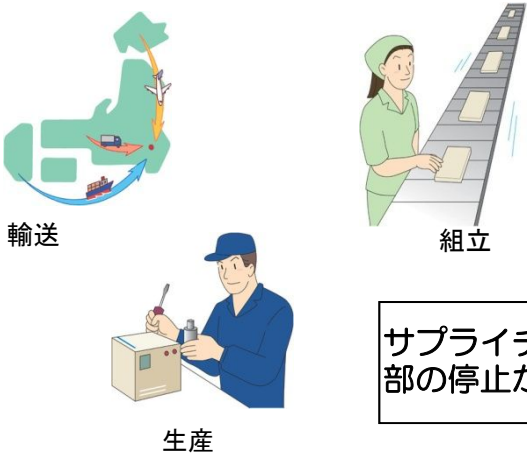
ＩＴサービス継続とは、必要な対策とコストとの見合いで最適な方法を見つける取り組み。

２．なぜＩＴサービス継続が必要なのか

近年、大規模地震や台風、ゲリラ豪雨など集中豪雨による洪水などの自然災害により、大きな被害が発生したというニュースを聞くことが多くなりました。また、新型インフルエンザの大流行により外出が制限されるようになる可能性についても考えられています。

また、大規模災害以外にも、火災や長時間の停電などの事故が発生する可能性もあります。

これらが発生した場合に、事業を継続することが困難になることが考えられます。



サプライチェーンの一部の停止が全てに影響

不測の事態が発生しても事業を止めない又はできる限り短い時間で重要業務だけでも再開する「事業継続」という観点が重要になってきています。

現在、大企業を中心に事業継続計画（ＢＣＰ）策定が進んでいて、取引先に対しても事業継続能力の向上について要請されることが多くなってきています。これは、例えば取引先の部品メーカーの業務が停止してしまった場合、自社の生産計画に影響が発生するからです。

実際に災害などが発生した時に事業継続を行うためには、平時のうちから準備してリスクに備える必要があります。

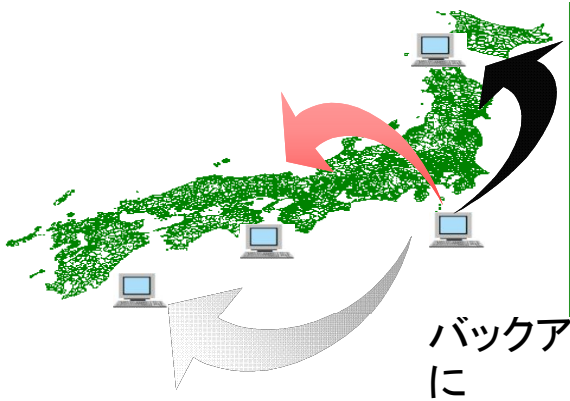
※阪神淡路大震災や新潟中越地震では、事業の縮小や廃業に追い込まれた企業もあり、甚大な経済被害を受けたことが知られています。しかし、事前に訓練まで行い、事業を早期復旧させた企業もありました。

近年、各企業では業務のＩＴ化が進展し、ＩＴサービス無くして業務の継続が難しいという状況になってきています。その為、重要な業務の継続を遂行していくためには、ＩＴサービスの継続能力を高めていくことが重要になっています。

逆に、事業継続計画を策定するために、まずＩＴサービス継続を検討するという考え方もあります。

コストとの兼ね合いになりますが、大規模災害が発生した場合でもＩＴシステムは、バックアップ施設を離れた場所に設置しておけば、そこからデータを参照することが可能ですので、他の生産設備とは異なり比較的復旧が容易であるともいえます。

ITサービス継続検討会議



バックアップを遠隔地に

事業継続のためにＩＴサービスの継続の検討が必要。ＩＴサービス継続のための検討を事前に行っておくことが重要。

３．ＩＴサービスの範囲

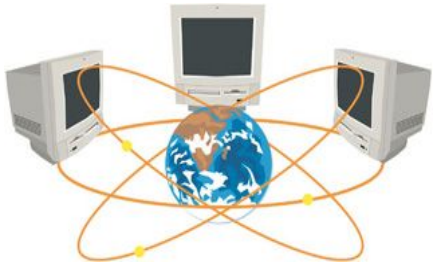
ＩＴサービス継続を考えていく上で、組織が使用しているＩＴサービスを洗い出す必要があります。洗い出したＩＴサービスについては、提供範囲はどこまでか、またサービスレベルはどのくらいかを明確にする必要があります。

つまり、どのＩＴサービスが組織のどの業務に大きな影響を与えるかを事前に調査しておく必要があります。

また、これにはＩＴサービスが依存している基盤となる共通のサービス（ネットワーク、電源設備、空調設備など）も含んで確認しておきます。

経理や人事

入力業務



ネットワーク

どのＩＴサービスが、どの業務に影響するかを、電源・空調・ネットワーク等のインフラも考慮して調査する必要がある。

ＩＴサービスの復旧が長引いても、手作業などの代替手段が存在し、一定期間内においてある程度のレベルで業務が継続できる場合があります。

逆にＩＴサービスの停止が即業務停止につながるような業務もあります。例えば電子メールシステムが停止してしまうと電子メールで注文を受けている業務は停止してしまいます。

このようにＩＴサービスへの依存度も明確にしておく必要があります。

最近はセキュリティ対策の為、ＩＣカードで入退室を制御しているオフィスが多くなっていますが、停電のときに入退室ができなくなる可能性など、通常は意識していないＩＴサービスについても調査しておく必要があります。

手作業での対応

電子メール受信

ITサービスへの依存度は

セキュリティ対応のオフィス

意識していないITサービス

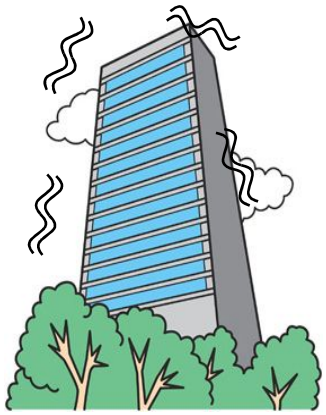
４．ＩＴサービス継続のために

（１）リスクの想定範囲

ＩＴサービス継続のためには、どのようなリスクがあるのか洗い出しを行う必要があります。大地震のような広範囲に及ぶリスクから、建物の火災などの内部の局所的なリスク、インフラ事業者の事故などの外部の局所的なリスクも含めて洗い出します。

リスクが想定されたら、その影響・結果についても想定します。例えば、建物の火災が発生するというリスクでは、火災場所でのシステム機器の損壊や電源系統の被害などが発生するかもしれません。

最近では、新型インフルエンザなどの伝染病の蔓延により、多数の従業員が欠勤するという要員不足のリスクやテナントビルの閉鎖といったリスクも考えられます。



地震や火災

外出制限

ＩＴサービス継続のために、まずリスクの洗い出しの検討が必要。

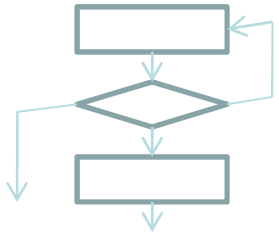
（２）事前に検討しておくべき事項

次のような事項を検討しておきます。

- 緊急時の対策本部体制
- 緊急時の連絡体制、連絡方法
- 安否確認方法
- 緊急時初期対応手順
- 業務影響を考慮したＩＴシステムの復旧優先度・依存度
- 重要システムの災害対策
- 代替機などの手配手順
- 代替要員手配手順
- ＩＴシステム復旧手順
- 新型インフルエンザへの対応計画

※　重要なシステムを稼動するために、優先度の低いシステムを停止するようなことも考えられます。

緊急対策本部の設置



復旧手順の明確化

必要事項の検討会議

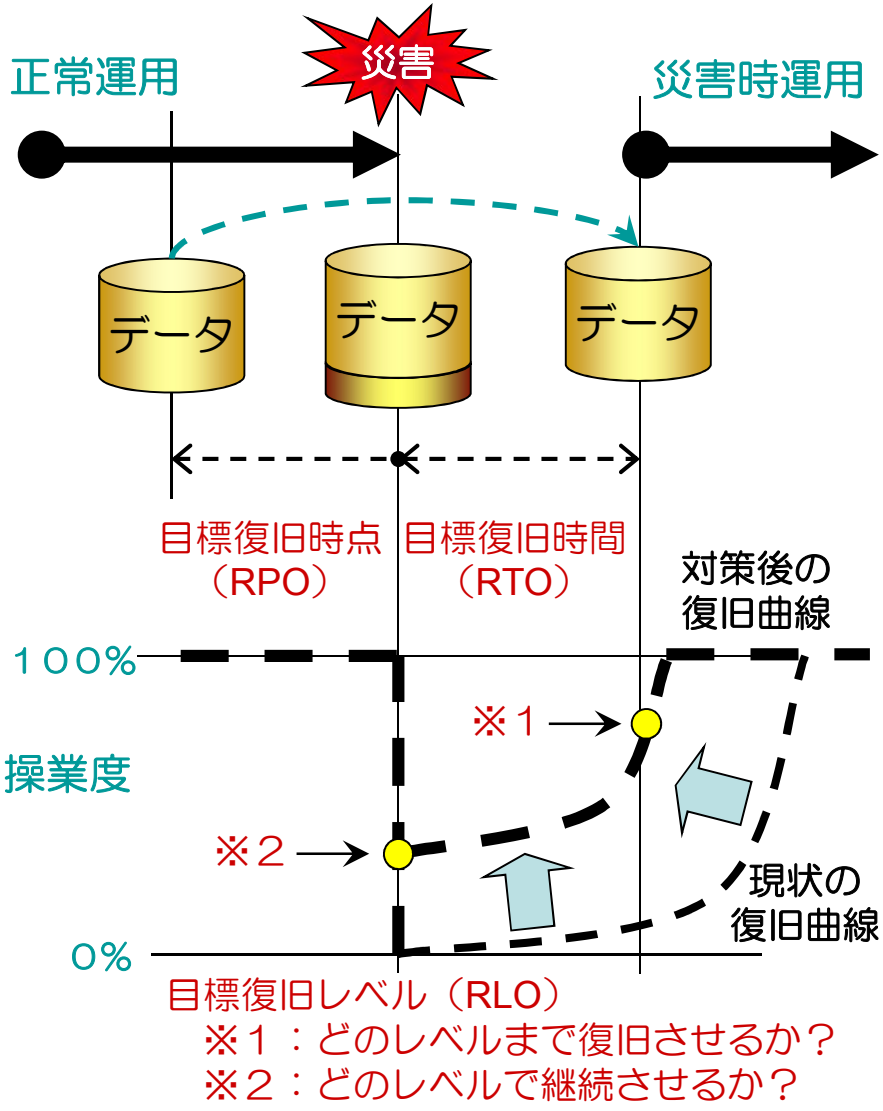
事業継続のために事前に検討しておくべき項目です。新型インフルエンザによる従業員の不足等も考慮が必要。

５．ＩＴシステム災害への対策

ＩＴサービス継続のためのＩＴシステムへの具体的な対策は、対策に必要な費用を考えた場合どのように検討していくべきでしょうか？

まずは、万が一の災害等が発生した場合を想定し、現在の事業の復旧を何時までに行わなければいけないのか？（目標復旧時間：RTO）、どのレベルまで復旧していないと業務を行うことができないのか？（目標復旧レベル：RLO）、また復旧すべきデータが何時の時点でなければいけないのか？（目標復旧ポイント：RPO）を検討します。これらは一般的に、事業継続計画（BCP：Business Continuity Plan）により設定されるものでもあります。

一般的には、目標復旧時間が短いほど、目標復旧レベルが高いほど、目標復旧ポイントが短いほど、それらの対策に必要な費用は高額になっていきます。設定した目標に合わせた対策とその投資をしっかりと行っていくことが必要です。



※　操業度：たとえば、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、
いくつの生産（処理）数まで復旧が必要か
いくつの生産（処理）数で業務を継続するか？
という目標を検討します。

現時点における業務のＩＴ依存度と、ＩＴサービスが停止してしまうと想定されるさまざまな脅威（リスク）を検討し、それぞれのＩＴシステムの重要度と目標である目標復旧時間、目標復旧レベル、目標復旧ポイントとを比較検討します。
それが業務影響分析（ＢＩＡ：Business Impact Analysis）です。そのＢＩＡにより明確になった、目標と現状との差をできるだけ小さくする為の対策を行っていくことが重要となります。

それでは、一般的に想定されるリスクとそれらの対策についてどのようなものがあるでしょうか？ここでは、災害を中心にご紹介します。

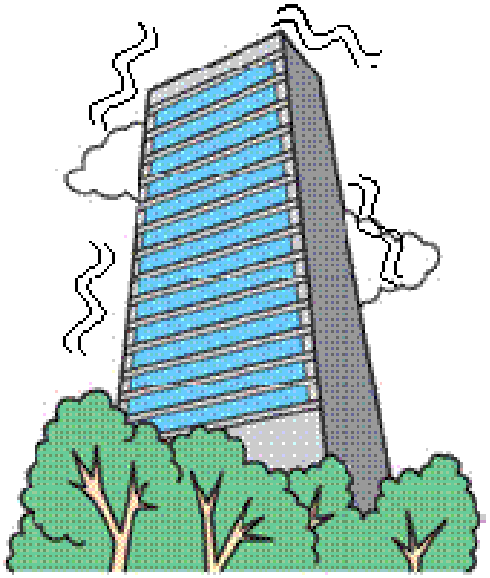
５．１　地震対策

（１）建物における対策

ＩＴサービスにおける重要なシステムがある建物について、特に1987年（昭和６３年）６月以前の建物。旧耐震基準による建物については確認をした方が良いでしょう。

（２）ＩＴシステム機器の耐震、免震装置の設置

ＩＴシステム機器の転倒や位置がずれたりする事により、ＩＴシステム自体や搭載ラックの損害やケーブルの断線等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等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／耐震対策等も比較的普及しています。これらの免震／耐震対策は、データセンタ等で採用されていることも多く対策の一つとして高い水準を確保することが可能です。



５．２　落雷対策

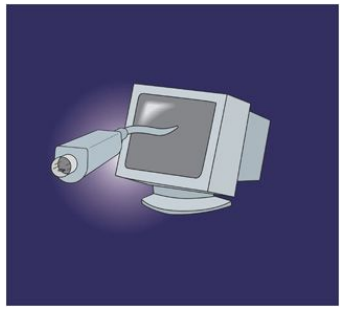
落雷による被害として電源関連が強くイメージされますが、昨今ではネットワーク等に対しても影響が発生するケースも少なくありません。基本的な電源への落雷対策をはじめ、ＬＡＮ／ＷＡＮなどのネットワークにおける対策もよく検討しておきましょう。これらの落雷対策は、接地（アース）強化をはじめ、防雷製品群は比較的普及しており、手軽に実施できる対策の一つです。

５．３　停電対策

落雷等による瞬間的なものから、一般的な停電に対する対策としてＵＰＳ（無停電電源装置）が普及しておりますが、一般的にこれらＵＰＳは、サーバ等を正常に終了させるまでの時間を確保することが一般的で、長時間の停電時にＩＴシステム機器を稼動させる為の目的ではありません。したがって、ＩＴサービスを継続させる為には発電設備が必要となる場合が一般的です。

これら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。

これらの非常用発電設備は、持ち運び可能なタイプから屋外設置型などが有り、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。



停電による
業務停止

ネットワークへの落雷による影響や、許容復旧時間にかかわる停電への対策準備が必要。

５．４　火災対策

　基本的にＩＴシステム機器にとって水は大敵です。したがって、スプリンクラや消防による消火の為の放水を避ける必要があります。
　その為には、ハロン系消火剤を準備する等あらかじめ消防署に消火方法について相談する等、万が一火災が発生した場合でも、ＩＴシステムに影響が少ない方法を検討したほうが良いでしょう。

５．５　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一つがバックアップです。

　企業の規模や業種などに関わらず、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、先に述べたように、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小さく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。

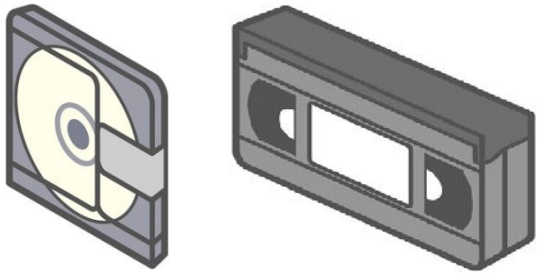
　逆に更新頻度の低いデータや、業務アプリケーションなどのＩＴシステム自体をバックアップするケースでは、比較的長い周期でバックアップを実施し、確実にデータを保管しておくことが重要となる場合もあります。

ネットワークを利用したバックアップ

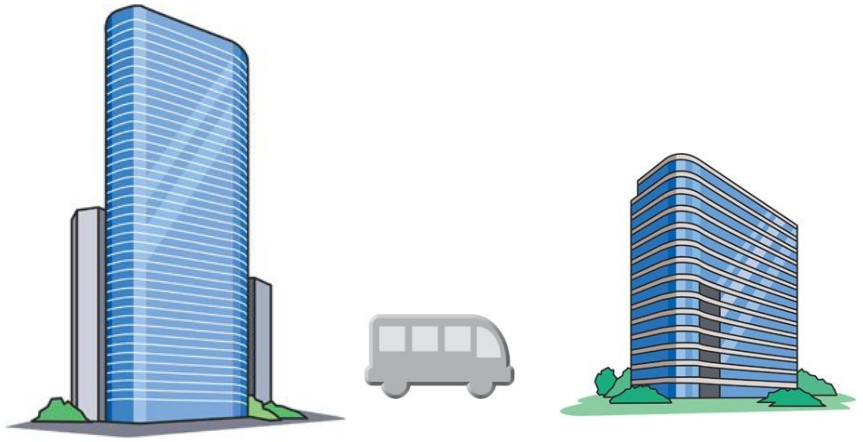
比較的長期間、データを確実に保存しておくためには、ディスクやテープなどの記録媒体が適していると考えられますが、目標復旧ポイントや目標復旧時間を短縮するためには、外部のサーバやストレージのような媒体に保管する方が一般的と言えます。

また、バックアップしたデータの保管場所も重要です。大きな災害を想定した場合には、遠隔地に保管する方が望ましいと言えますが、保管場所までの移動手段や移動時間など、目標復旧時間を考慮した検討が必要です。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する場合や、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。

以上のように、システムの重要性に応じたバックアップ設計を行った上で、それぞれに最適な手法を選択する事が、効率よく効果的なバックアップを行うポイントとなります。



バックアップの形態や保管場所、復旧方法は、システムの重要性に応じて対応することが効果的。



遠隔地での重要データ保管

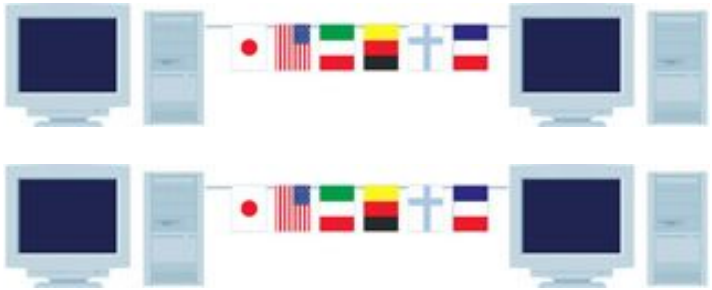
５．６　二重化（冗長化）

　ＩＴシステム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するため、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ために、予備のシステムを用意しておくことを二重化と言います。

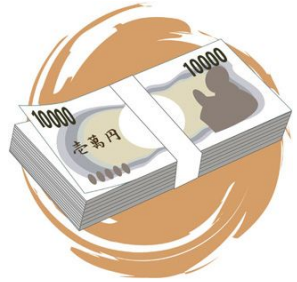
　ＩＴシステムやネットワークに関わる全ての機器を二重化できれば理想的ですが、そのためには膨大なコストが必要となるだけでなく、システム構成が複雑化するという弊害もあります。

　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システムの二重化もサービス継続には有効だが、大きなコストがかかることへの考慮が必要。



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る。

６．ＩＴシステム運用面での対策

日々の業務を行ううえで重要な役割を担っているＩＴシステムは、対応する業務範囲が大きくなり、より重要な業務が行われる様になっています。これらのＩＴシステムの安定稼動を行う為の「運用」に携わる担当者が必要です。また、ＩＴサービス停止時を想定した、運用における対策について以下に説明します。

６．１　ＩＴシステム運用担当者

ＩＴサービス停止時を想定し、ＩＴシステム運用担当者をはじめ全従業員の緊急事態発生時の安否確認はもとより、ＩＴシステムの復旧に携わる運用担当者や関連する組織の担当者の氏名や連絡先が明記された「緊急時体制リスト」を作成しておきましょう。また、災害時や新型インフルエンザなどにより、運用担当者が対応できない場合の「代替要員」についても明確にし「緊急時体制リスト」に加え、平時からしっかりと教育等を実施しておきましょう。

「緊急時体制リスト」の作成や、ＩＴシステム運用担当者が対応できない場合の代替要員の確保と教育も重要。

６．２　ワークスペース

　緊急事態発生時等においてＩＴサービスを継続さえるためには、その継続や復旧作業を行うワークスペースが必要になります。このワークスペースは、平時においては特に必要でないため、あらかじめ必要な設備や作業場所を計画・確保しておく必要があります。なお、目標復旧時間や被害軽減対策などにより、その要員・設備・広さなどを見積る際に大きく影響します。また、ＩＴシステムやバックアップの形態によっては、自分達の組織内ではなく、外部の組織との契約によって、そのワークスペースを確保する場合もあります。しかしながらこれらの場合も、事前にＩＴサービス継続計画にもとづき平時より契約されていることが前提であり、緊急事態発生時にあらたに契約する事はできません。

６．３　外部のＩＴサービス

　外部のＩＴサービスを利用している場合で、ＩＴシステムの一部に外部サービスを利用している（データセンタ等）場合は、ＩＴサービスを提供している外部組織における事業継続計画の確認や監査を行う事が重要になります。

ＩＴシステムが被害にあった場合の代替機や代替スペースを明確にしておくことで、業務復旧までの時間を短縮することができる。

６．４　サービスレベル管理

　ＩＴサービスが停止してしまった場合や処理速度の低下などにより、平時と同様な処理が行えないために業務処理にかかる時間が長くなることが予想されます。そのようなＩＴシステムの稼働状況に応じた各業務システムのサービスレベルについて、あらかじめ想定しておくことが必要です。

６．５　テスト・点検

　ＩＴサービスが停止してしまった場合に備え、あらかじめＩＴサービスの復旧手順に関するマニュアルを整備する事はもちろんの事、業務やシステム単位での優先順位などを明確に定めておくことが必要です。また、要員の異動に伴う緊急時体制リストの更新やＩＴシステム機器（サーバ、ネットワーク機器やオペレーティングシステム、業務アプリケーション等々）に変更があった場合など、作成されている手順書等の更新が適時行われている必要があります。さらには、ＩＴサービスが停止している間、業務を継続するための代替手段（手書き伝票やFAXの使用等々）を準備しておくことも重要です。

一般にＩＴサービスは、物理的な実体のある製品に比べて、サービスの内容と範囲、品質が分りにくい為、重要な内容を数値化し明示的・定量的に定義しておくと良い。

代替手段の準備

ＩＴサービス継続のための各種手順を明確にし、かつそれを定期的に見直ししておく事が必要。

また、実際のＩＴサービスの停止が極めて稀な非日常であるため、平時より、復旧や被害拡大を防ぐために計画の実効性を確認しておくことが必要となります。経済産業省作成の「ＩＴサービス継続ガイドライン」ではテストの種類と概要を以下の様に分類しています。

（１）机上チェック
作成された計画内容を関係者がそれぞれ確認することです。
（２）ウォークスルー
作成された計画内容を関係者が集まり読み合わせを行いながら有効性を確認することです。
（３）シミュレーション
あらかじめ設定されたＩＴサービス停止の状況における対応を行うことで、有効性の確認を行います。
（４）ロールプレイング
あらかじめ設定されたＩＴサービス停止の状況において対応を行う中で、新たな未設定の状況を付加しながら、有効性の確認を行います。
（５）実機確認
実際の設備を用いた対応を行い、計画や手順書等の有効性の確認を行います。

ITサービス継続計画の実効性はOKですか

ここではＩＴサービス継続計画の実効性を検証するために、テストの種類と概要を示している。より詳細については「ＩＴサービス継続ガイドライン」参照。
ＵＲＬは次の通り
http://www.meti.go.jp/press/20080903001/20080903001.html

さらに、テストでは下記内容が検証されることが望まれる。としています。

・代替システムにおけるバックアップ媒体からの復旧手順書等の確認

・復旧チーム間の共同作業の内容や手順の良否等の確認

・組織内及び組織外とのシステム接続の良否等の確認

・代替装置のシステムの性能も含めた実用性の良否等の確認

・通常システムへの切戻し手順の良否等の確認

・通常業務の復旧手順の良否等の確認

・組織内外への連絡・通知手順の良否等の確認

復旧手順書・手順の確認

ＩＴサービス継続の為に、通常では殆どやらない手順で操作や確認を、間違いなく行うためには、定期的に実際に行ってみることが重要。また、外部環境の変化による手順の見直しも定期的に行っておくことが、災害等発生時の迅速な復旧につながる。

６．６　監査

運用対策としての監査の意義は、ＩＴサービス継続計画の運用的対策の整備状況及び運用状況について客観的評価を実施することにあります。「ＩＴサービス継続ガイドライン」では、下記の項目について言及されています。

（１）リスク評価に基づき策定されているか？

（２）リスクに対応してそれを統制、提言するものとなっているか？

（３）計画に含まれる事前対策計画は適切に整備運用されているか？

（４）事後対応計画は適切に整備され、実施可能なものとしてテスト・訓練が行われているか？

（５）外部委託先についても整備、運用が講じられているか？

客観的評価でも
問題なし！

ＩＴサービス継続のための事前対策計画の適切な運用と、事後対応計画の整備・テスト・訓練が、確実になされているかを定期的にチェックすること等を監査という。

７．ＩＴサービス継続への対策

７．１　点検評価

（１）ＩＴサービス継続計画の点検評価の重要性

　ＩＴサービス継続計画は、策定し体制を構築すればそれで終わりではありません。企業の経営方針や組織の役割、企業を取巻く環境や相互の作用により、その内容は陳腐化していきます。

　多大な労力と費用をかけて構築した体制が、いざというときにきちんと機能しなければ、逆に企業に損失を与える結果につながる事もあります。

　そのため、構築したＩＴサービス継続計画の体制は、定期的に点検評価することによって、その内容が企業の現状にとって妥当であるか、正常に機能するかを確認することが重要となってきます。

作成構築

点検評価

見直し・再構築

ＩＴサービス継続計画構築後は、定期的に点検･評価･再構築を繰り返すことによって機能を維持することができる。

７．２　対策検討

（１）ＩＴサービスの中断・停止による経営への影響

現代の企業活動は、ＩＴへの依存性が高まり、ＩＴサービスの中断・停止は、時に業務に多大な影響を与え、社内の利用者のみならず、取引先や顧客にまでご迷惑をかけることもあります。

そのため、ＩＴサービスの中断・停止が各業務に与える影響を分析し、その業務が中断・停止となった場合の経営に与える影響を検討することが必要です。

また、検討の際には、在庫管理システム、販売管理システムといった、具体的なシステムの検討だけでは、不十分です。それらが依存している基盤となる共通のＩＴサービス、例えばＬＡＮや通信回線等についても配慮を行う必要があります。

事業継続が企業の重要な経営課題であり、社会的責任であるとすれば、ＩＴサービスの中断･停止に備える「適切な管理策の整備」もまた、重要な経営課題のひとつといえます。

業務への影響を分析

経営への影響を検討

適切な管理策を整備

必要なＩＴサービスの継続には、企業経営の観点からも「コストをかける」。結果的に重大な損失・損害を抑えることができる。

（２）ＩＴサービスが中断・停止した場合の復旧目標（時間・データ・レベル）

復旧目標としては、次のものがあります。

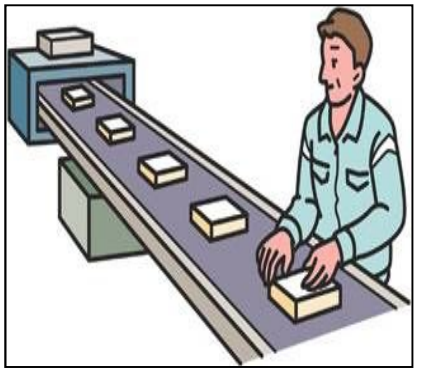
・目標復旧時間
　復旧までの目標時間
・目標復旧ポイント
　データの復旧目標ポイント（どの時点のデータまで復旧させるか）
・目標復旧レベル
　本格復旧前の暫定業務の実施（最低限の業務の再開･継続）に必要なレベル

　ＩＴサービスの適切な継続を実現するには、上記のような復旧目標を検討し、それが可能なように準備しておくことが必要です。

　ただし、復旧目標を高くすれば、一般的に必要コストも高くなるので、そのＩＴサービスを利用している業務に対する影響度とコストを勘案して対策を立てることが必要です。

ＸＸ時間以内に復旧

ＸＸまでのデータ復旧



通常のＸＸ％まで復旧

「時間」？　「データ」？　「レベル」？
適切な「復旧目標」をたてているか？

（３）ＩＴサービスの中断・停止を引き起こす原因への対策検討

ＩＴサービスの中断・停止を引き起こす原因としては、次のようなものがあります。

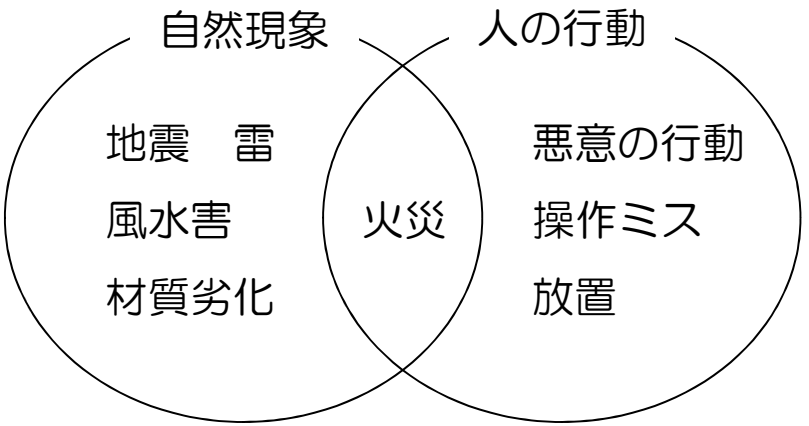
・自然現象（災害、物理的現象）
　地震、雷、風水害、火災・・・
　材質劣化、材質疲労、変質、風・・・
・人の行動（故意、過失）
　悪意の行動、破壊、放置・・・
　疲労･能力不足等による操作ミス・・

適切な抑止･予防管理策を整備できれば、上記のような原因の発生および実害を低減でき、ＩＴサービスの適切な継続が可能となります。

ただし、その発生を完全に防ぐことは困難です。抑止・予防の管理策と同時に、早期発見・修復といった、損失・損害を限定する管理策の整備にも力を入れることが必要です。

原因ごとに抑止・予防・発見・修復のどの管理策を重点的・複合的に整備するのが適切か、適時検討することが望まれます。

［原因の種類］



［管理策の種類］

事前対策	抑止	原因の発生を抑制する
	予防	原因が発生しても障害（中断・停止）に結びつかないようにする
事後対策	発見	障害の発生を検知し、通知する
	修復	障害による損失を限定する 正常な状態に回復する

自然現象と人の行動。それぞれに対して適切な管理策を立てているか？

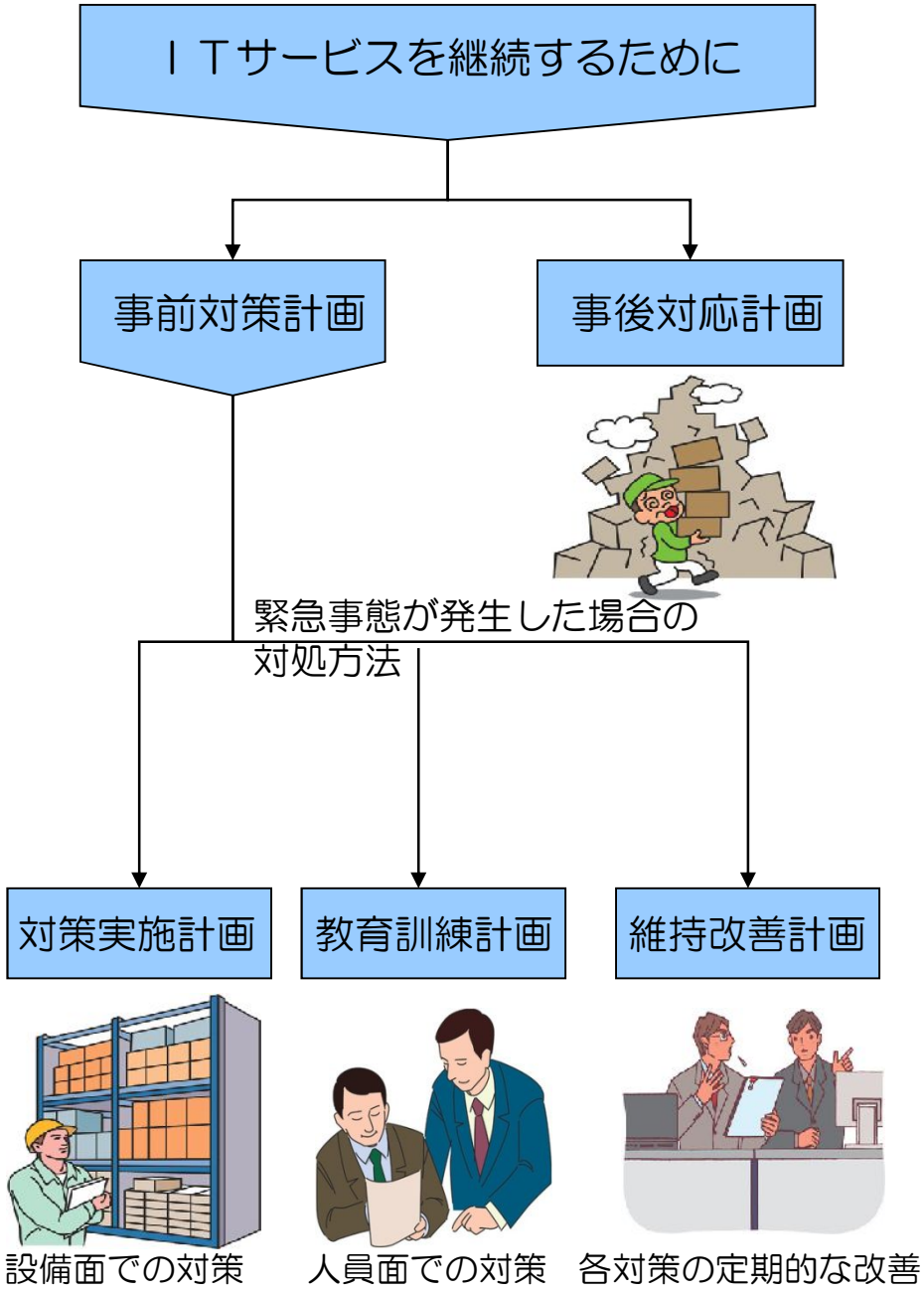
７．３　計画立案

　ＩＴサービスの適切な継続を実現させるために、事前の対策及びＩＴサービスの継続を妨げるような緊急事態が発生した場合における具体的な対応方法・計画を取りまとめて文書化する必要があります。

　ＩＴサービス継続計画としては、以下のものがあります。

①事前対策計画
　バックアップの設定、社員の教育など、緊急事態が発生することを前提として、被害を軽減するための計画です。

②事後対応計画
　ＩＴサービスが中断・停止した場合に、業務に深刻な影響を与える前に復旧再開するための計画です。



（１）事前対策計画

事前対策計画には、以下のものがあります。

・対策実施計画
　バックアップシステムの構築や、データバックアップの実施、サーバルームなどの耐震強化といった設備面での対策を定めます。

・教育訓練計画
　ＩＴシステムの担当者の意識、対応能力の向上のために教育訓練を定めます。

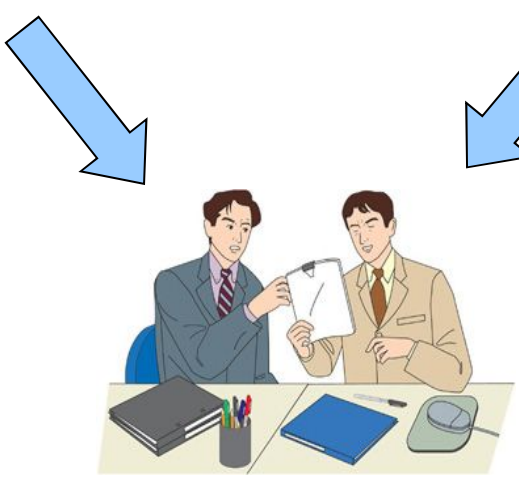
・維持改善計画
　定期的なテストによる各対策・計画の評価、改善の実施を定めます。

その他、従業員の安否、作業場所、外部サービスとの連携なども考慮する必要があります。

各計画の実施・監査を滞りなく進めるためには、費用面や教育訓練に対しての経営者側の理解が必要不可欠です。

［事前対策計画］

設備投資　　関係者の教育



定期的にテストを行い、結果をもとに各対策・計画の改善を行う

ＩＴサービスの中断・停止を避ける、または中断・停止した際に被害を最小限に抑える。

（２）事後対応計画

事後対応計画には、以下のものがあります。

・緊急時対応体制
　緊急事態に設置する対策本部や、要員の連絡方法と連絡先などを記載します。

・緊急時対応プロセス
　緊急事態における対応過程を定めます。特に緊急事態における、バックアップシステム（代替手段）への切替えなどの基準や、発動者の決定が重要です。

・緊急時対応手順
　担当チームごとに、各過程における、対応手順の詳細を定めます。

　また、緊急事態において、ＩＴサービスを継続を優先するために、実際の担当者に判断を委ねることによるセキュリティ水準の低下についても、検討しておく必要があります。

［緊急時対応プロセス　例］

①．対策本部に要員を召集被害評価

②．あらかじめ定めておいた代替手段による運用

③．機能復旧後、代替手段からの切り戻し

［緊急時対応手順　手順書例］

・バックアップシステム切替え手順書
・バックアップシステム運用手順書
・バックアップデータ管理リスト
・ネットワーク復旧手順書
・対応項目チェックリストなど

緊急事態が発生したときに、復旧までの過程、手順をまとめておけば、被害を最小限に抑えることができる。

８．ＩＴサービス継続対策について

ＩＴサービス継続を支援するために様々なサービスメニューがあります。ＩＴサービス継続対策となる支援メューについては以下のようなメニューがあります。

（１）ファシリティ

ＩＴサービス継続するためには、ＩＴ設備などを、効率的に管理し自然災害などからＩＴ機器を保護する必要があります。以下のような対策をファシリティと総称します。

・自家発電電力供給
災害発生時など電力供給が止まったときに自家発電装置を用意し電力供給をすることでＩＴサービス継続対策となります。

・受電ルート二重化
ＩＴ機器を作動させるために必要な電力の供給ルートを二重化することにより、１ルートの電力供給が遮断されても、ＩＴ機器の動作を確保することが可能です。

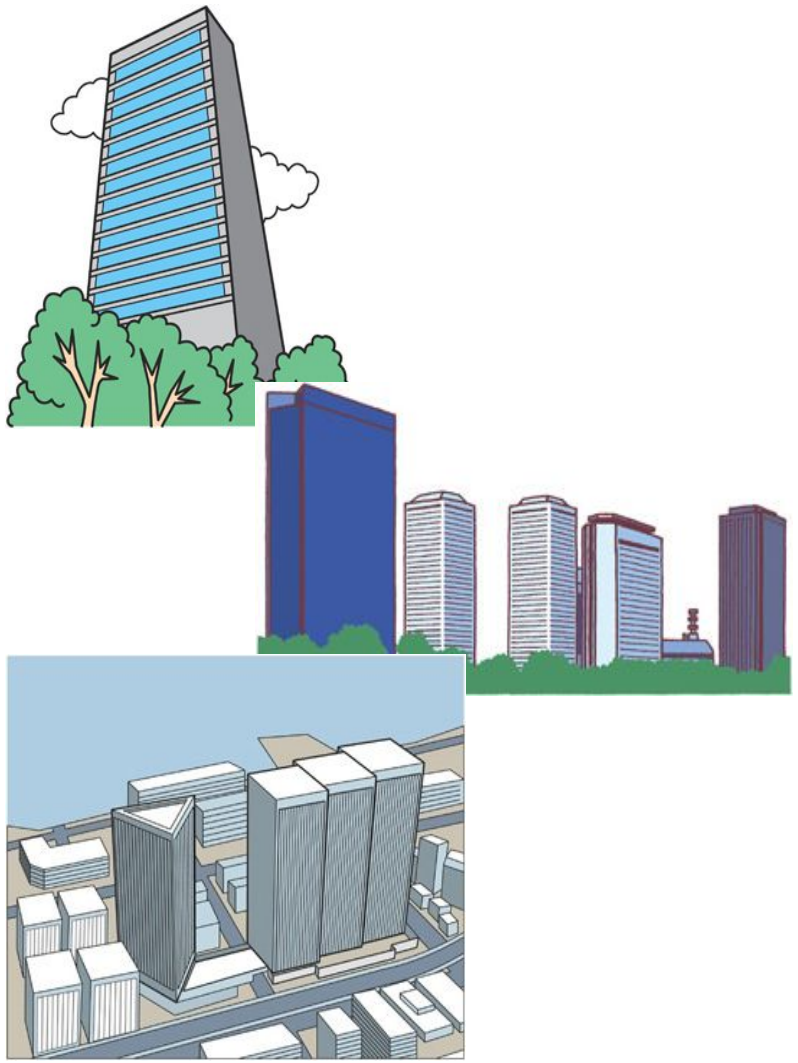
ＩＴサービス継続対策の様々なサービス

自家発電電力供給
受電ルート二重化

・免震床、ビル
免震床は、地震の揺れからＩＴ機器を守るため揺れを防ぐ構造を床に施した対策です。
また、ビル自体が免震構造になったビルで重要なデータを管理するデータセンタなどは免震構造が一般的です。

・避雷ビル
雷からＩＴ機器とビル自体を守る対策をしているビルを避雷ビルといいます。
落雷などの影響で、瞬間的に高電圧が発生することを雷サージといい、雷サージからＩＴ機器や通信回線を守ることはＩＴサービス継続対策のひとつです。

・自動消火設備
火災を監視する設備で火災を感知すると自動的に消火する設備です。
火災発生時にＩＴ機器の被害を最小限に留める対策となります。



免震床、避雷、自動消火などの対策

（２）データセンタ　アウトソーシング

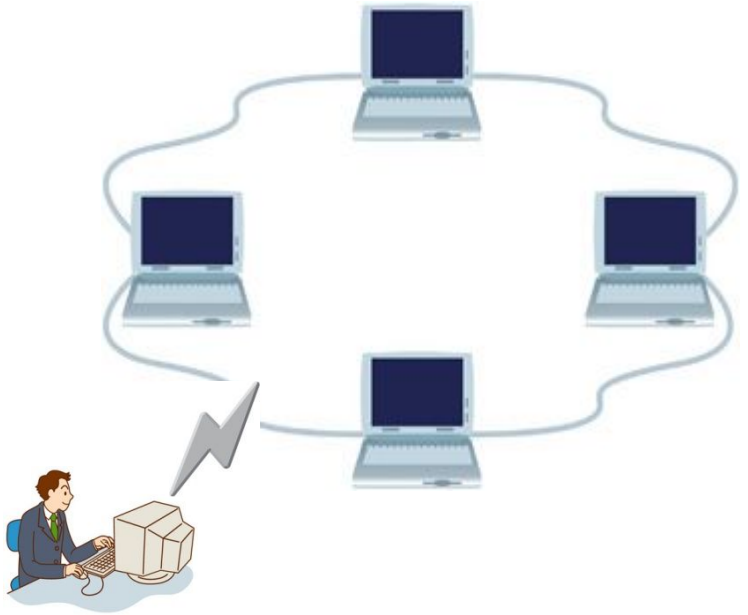
・ＡＳＰ(ApplicationServiceProvider)
ユーザーが必要とするシステムの機能を、ネットワークを通じ提供するサービスです。

・ＳａａＳ（Software as a Service）
ライセンスを購入し、必要な機能を有料で利用できるサービスです。

・クラウドコンピューティング
（Cloud Computing）とは、ネットワーク上のサーバを意識することなくインターネット接続し必要なサービスを利用できる形態をいいます。ネットワークを雲のように図示することでクラウド（雲の名前の由来となっています。ＡＳＰ、ＳａａＳも、クラウドコンピューティングのひとつといえます。

上記のサービスは、システムの機能が自社に存在しないため、ある地域が災害となった場合も他の地域でシステムを利用できるメリットがあり、ＩＴサービス継続に有功です。

・ASP
・SaaS
・クラウドコンピューティング



ネットワークを利用したサービス

以下のサービスのように、各種対策設備等の整ったベンダのコンピュータを利用することで自社での、各種障害へのリスクを軽減することが出来ます。

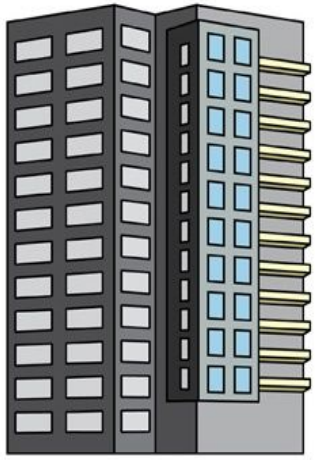
・ハウジング
自社で準備したサーバ、コンピュータを回線や電源設備が整ったベンダーが、運用するセンタが預かるサービスです。

・ホスティング
ベンダーがセンタに準備した、サーバやネットワークなどの機器の容量や機能の一部を利用するサービスです。
ハード購入の必要がなく、システム運用もベンダ側で行います。

・リモートバックアップ
重要なデータをネットワーク網を利用し遠隔地にバックアップするサービスです。

・サーバ共用サービス
１台のサーバを複数の人や企業が利用するサービスをいいます。
サーバを複数で利用するためコスト削減効果があります。ただし動作が遅いなどデメリットもあります。

・メインフレーム共用サービス
企業の基幹業務に使われる汎用大型コンピュータをメインフレームといいます。
メインフレームのハードウエアを分割し共用するサービスです。
コスト削減効果と効率化がメリットです。



ハウジング／ホスティングなどの
ＩＴサービス継続対策

（３）耐災害対策（設備）

　万が一の災害に備える物理的対策においてサーバルームなどの設備ごとに対策が可能なものがあります。

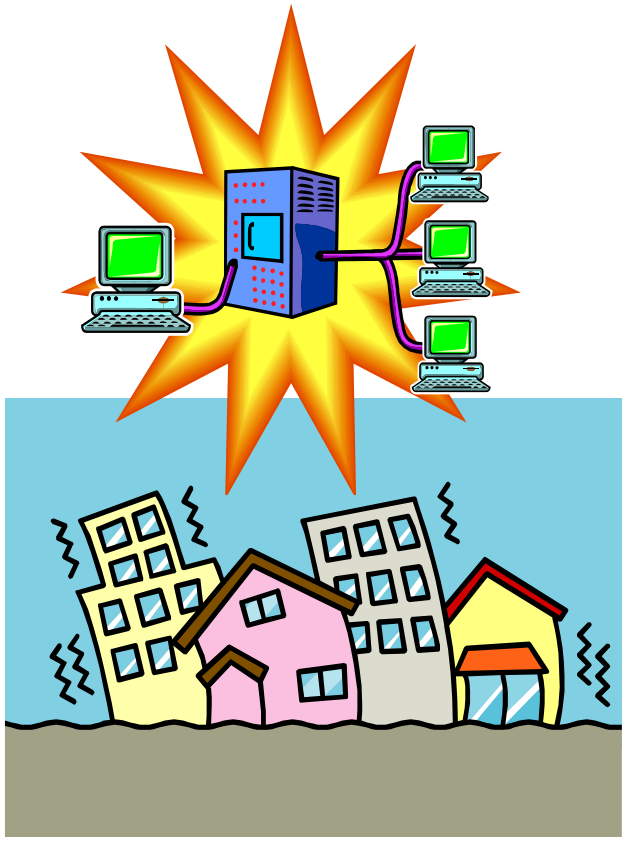
　設備対策には主に下記のような種類があります。

・免震床
　ラック免震床全体やラック～床間に免震装置を設置して、地震による被害に備えます。

・消火設備
　火災に備え、水消火や粉末消火等、システム設置場所の環境や用途に応じた消火設備を設置します。

・ＵＰＳ設備
　停電発生時に備えた適切なＵＰＳ配置や長時間の停電にも対応が可能な発電機の設置を行ないます。

災害時の対策が重要！



（4）耐災害対策（システム）

設備対策に対し、システム単位で行なえるＩＴサービス継続のための物理対策には、下記の種類があります。

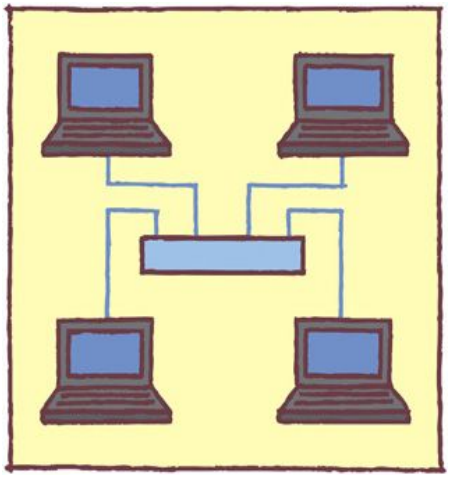
・ホットスタンバイシステム
同じ構成のシステムを２系統用意しておき、片方を作動させ、片方は同じ動作を待機状態にしておく対策方法です。
障害発生時は、即座に待機系に切り替えるためダウンタイムが短縮できます。
設備対策に対し、システム単位で行なえる物理対策には、下記の種類があります。

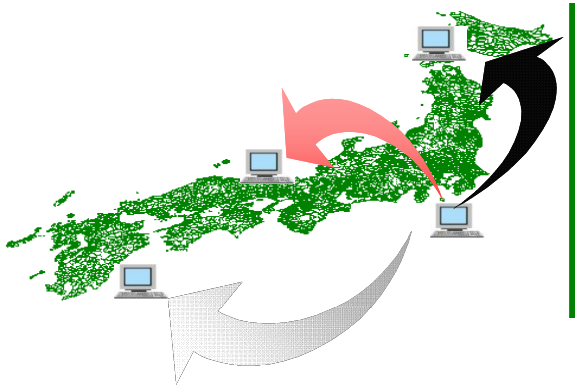
・コールドスタンバイシステム
ホットスタンバイに対して、主系と待機系の同期を行なわず、主系に障害が発生してから待機系を作動させる方式をコールドスタンバイ方式といいます。

・リモートバックアップ
バックアップデータを自動または手動で遠隔地のデータセンタなどに保存することができるサービスです。

・バックアップ媒体外部保管
媒体に保存されたバックアップデータを遠隔地のデータセンタ等に保管します。

ホットスタンバイシステム
コールドスタンバイシステム
による災害対策





遠隔地へバックアップ

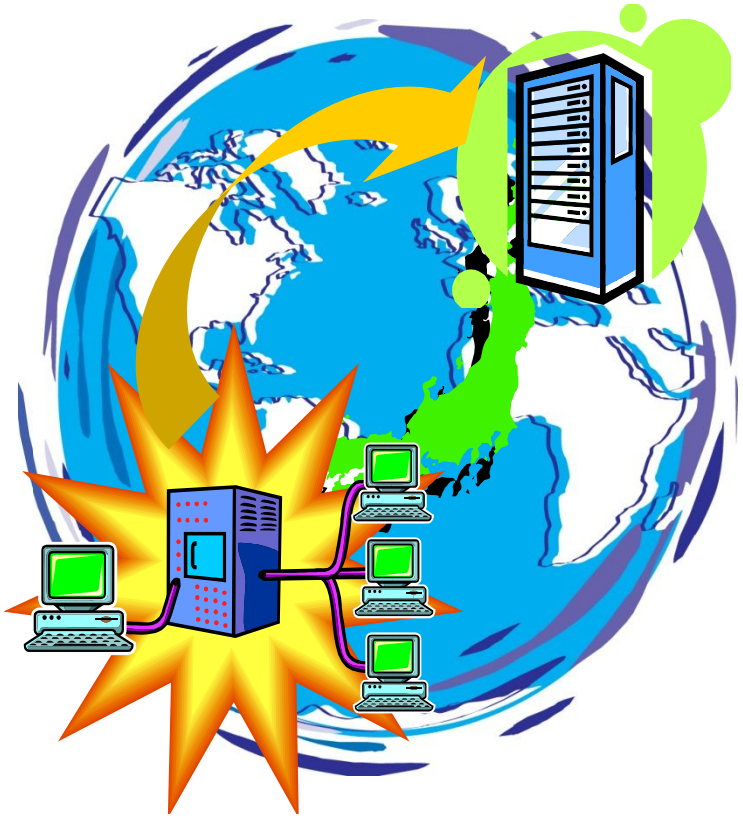
（5）代替システム対策

　業務のダウンタイムを軽減するため、予め予備機を準備しておき、災害時に利用することができるサービスです。

・代替システム
　同一構成システムを別のデータセンタ等に準備しておき、被災地のシステムがダウンした際に、復旧までの間利用することができます。

・代替ＰＣ
　使用しているＰＣの障害発生時に、予め用意された社内標準ＰＣ（基本ソフト等を導入済みの代替機器）と交換し、復旧までの間利用することができます。

代替システム対策



（６）代替ネットワーク対策

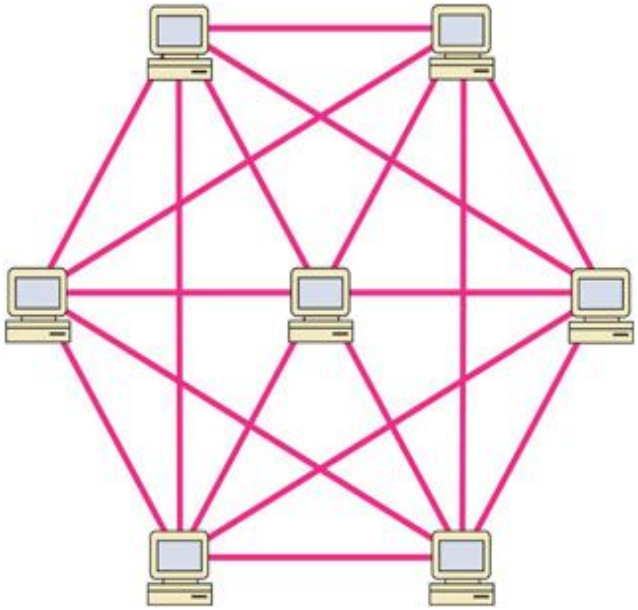
様々なＩＴシステムの共通基盤となるネットワークインフラについて、複数構築（冗長化構成）することにより、広域災害やネットワーク障害発生時の通信経路を確保し、業務を継続することを可能にします。

・通信ルート二重化
平常時に利用するネットワークに対し、バックアップとなるネットワークを契約しておき、被災時には迂回ルートとして利用できるサービスです。
また、基幹系と情報系など、用途別に通信ルートを分けておき、相互にバックアップ可能にしておく方法もあります。

・引き込みルート二重化
建物構内への回線の引き込みルートを、東西や南北などのように物理的に分けることが可能な場合、被災箇所を迂回したルートを利用することができます。

・ルート切り替え
代替システムのあるセンタ側で、通信ルートの切り替えを行ないます。

代替ネットワーク対策



（7）セキュリティ

ＩＴシステム全般における様々な脅威に対して、規制や保護を行うサービスを指します。

・ホームページ改ざん対策
情報システムの脆弱性を悪用してＷＥＢサーバへ不正に侵入し、ホームページの改ざんをする攻撃に対しファイアオール（防御壁）や最新のセキュリティプログラムを導入し脆弱性を排除する対策を指します。

・ウイルス監視、駆除
ＷＥＢ閲覧やメールの添付ファイル等を介してウイルス侵入することを防止し、システムの破壊や情報漏えい等の活動を行わない様に対策が必要です。
アンチウイルスプログラムやウイルス検出装置を導入する事で、ウイルスの侵入防止・活動の停止・削除／隔離等対策することを指します。

様々な脅威から防御

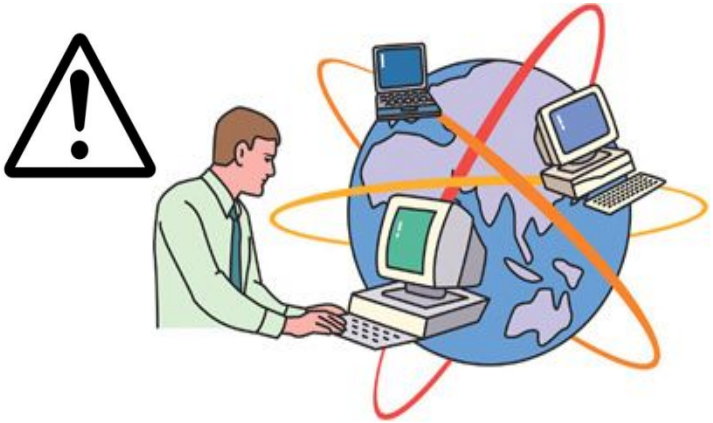
・サイバーアタック対策
情報システムの脆弱性を悪用してシステムへ不正に侵入し、データの改ざんや窃取・システムの破壊をするものや、大量の電子メールの送付・掲示板への無差別書込など、システムの機能不全を目的とした攻撃を防ぐため、ファイアウォール（防御壁）や最新のセキュリティプログラムの導入を行い、脆弱性を排除する対策を指します。

（8）アウトソーシング

様々な業務を外部へ委託することで業務の効率化や管理工数の削減をすることができるサービスを指します。ＩＴサービス継続のためのリスクの軽減や復旧時間の短縮に有効です。

・ヘルプデスク
システムの使用方法に対する問合せや、トラブル発生時の対応等に対する窓口を開設するサービスです。

専門家が対応することにより、迅速な問題解決を行うことが可能です。



ネットワークを介した攻撃から防御

専門家によるヘルプ対応

・システム・オペレーション
サーバの起動／停止や、定期ジョブの実行、バックアップ運用、帳票運用などの定型的なオペレーション業務を、お客様の代わりに代行するサービスです。

・システム監視
システムの稼働状況を監視し、システム障害・ネットワークへの不正接続等を検知／診断／通報するサービスです。

・システム運用支援
導入したシステムを停止する事無く運用できるよう、技術的支援を実施するサービスを指します。

システム監視や運営支援

（9）コンサルティング／支援

ＩＴ設備導入に関する計画策定・情報提供を受けられるサービスを指します。

・ＩＴサービス継続計画策定支援
災害等により、ＩＴサービスを用いた業務が停止する事による、ビジネスインパクトを未然に防ぐ為、対応策を検討する為のコンサルティングサービスを指します。

・緊急連絡、安否確認システム構築
災害時にも回線障害の影響が少ない電子メール等の機能を使用して、迅速に緊急連絡・安否確認が行えるサービスを指します。

・システム対災害化設計・構築
地震・落雷・火災等の災害を受けた場合でも、被害を最小に留め、迅速に復旧できるよう設計・構築するためのサービスを指します。

・ＩＴサービス継続計画運用支援
ＩＴサービス継続計画に基づいたサービス導入後の運用・見直しを継続的に支援するサービスを指します。

コンサルティング

緊急連絡、安否確認システム構築

本解説書は下記の方々のご協力により作成しました

太田　和宏	日本事務器株式会社
大島　章宏	日興通信株式会社
小原　芳和	株式会社富士通エフサス
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
地神　明寛	株式会社ブロードリーフ
土渕　純一	株式会社大塚商会
野村　一平	株式会社ビジネスコンピュータ
芳賀　明夫	株式会社大塚商会
伴野　浩之	日本事務器株式会社
藤本　昌宏	株式会社シー・シー・ダブル
前場　宏之	トレンドマイクロ株式会社
森　　達矢	ＮＥＣフィールディング株式会社
加藤　　誠	日本コンピュータシステム販売店協会
山田　勝正	日本コンピュータシステム販売店協会

やさしい「ITサービス継続」

発行　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　鴫原ビル2階
電話　03－5802－3198
ホームページ　http://www.jcssa.or.jp

発行日　　平成21年9月（初版）

JCSSA