IT サービス継続ガイドライン

平成２０年９月

経済産業省

目次

注：
本文中において、『事業継続計画（BCP）策定ガイドライン[METI.1]』などの記述がある場合、『[METI.1]』は「6. 参照基準」に記載された文書への参照を意味している。

1. 背景と目的

1.1 背景

情報処理技術やネットワーク技術の発達と低コスト化が進む中で、現代の社会経済は、情報技術（IT）を活用することで、時間・空間を超えたサービス・商品の提供や、業務の効率性向上、意思決定支援などの分野での利便性を享受している。

一方で、IT への依存関係が急速に増大している現状においては、その潜在リスクや依存関係に起因する脆弱性を認識することが重要である。利便性を優先して、このリスク等に能動的な対応を行わない場合、何らかの IT 障害を起因として、IT に依存している個別組織の業務や、その組織が提供する商品・サービスの利用者、さらにはサプライチェーンやネットワークを介して国内外の社会経済にまで影響を及ぼすこととなる。また、実際にこのような事例も既に発生している。

IT サービスの継続性を確保することは、必ずしも事業継続性を全て担保するものではないが、先に述べた IT 依存関係の増加傾向を勘案すれば、事業継続マネジメント（BCM）の中から IT の要素を取り出して、IT サービスのマネジメント体制を事故前提の考え方に基づいて構築・維持していくことは、これからの安心・安全な社会の実現にとって必要不可欠である。

1.2 目的

経済産業省では、平成 17 年、事業継続計画の基本的な考え方から具体的な計画の構築手順までを解説した「事業継続計画（BCP）策定ガイドライン」[METI.1]を取りまとめた。同ガイドラインは、「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提に立った上で、事業継続は企業の社会的責任にも関係する問題であるとの考えから策定したものである。

同ガイドライン公表後も、我が国における事業継続への関心は高まっており、「世界最高水準の『高信頼性社会』実現」に向けた一要素として、事業継続の必要性はますます増大しているといえる。

しかし、「事業継続計画（BCP）策定ガイドライン」は、計画策定といったいわば高次の内容に焦点を絞っていることから、現場の立場から見た場合、同ガイドラインを使用することで高度な事業継続のための対策を直ちに策定できるとは限らないという一面があった。また、BCP を策定する企業の数は増加してはいるものの、未だその割合は十分とはいえない

状況にある他、前述した IT への依存性の増大もあり、事業継続の阻害要因として IT 関連のトラブルを挙げる企業の数は非常に多い。

このような背景から、本「IT サービス継続ガイドライン」は、「事業継続計画（BCP）策定ガイドライン」の IT にかかる部分について、企業をはじめとするユーザ組織を念頭に実施策等を具体化するものとして策定に至ったものである。

本ガイドラインは、組織[1]における IT サービスの企画、開発、調達、導入、運用、保守などに携わる部門[2]や担当者[3]が、事業継続マネジメント（BCM）に必要な IT サービス継続を確実にするための枠組みと具体的な実施策を示し、取り組みの実効性の向上を支援することを目的とするものである。

1.3 本ガイドラインの位置づけ

「IT サービス継続ガイドライン」は、経済産業省「事業継続計画（BCP）策定ガイドライン」の IT にかかる部分について、組織における実施策等を具体化したものである。本ガイドラインはその性格上、「事業継続計画（BCP）策定ガイドライン」と一対を為すものであるが、既に他の各種基準・ガイドラインを活用して BCP を構築している、もしくは構築を検討している組織においても、本ガイドラインを活用して、IT に関する事業継続に向けた体制についての検討を行うことが可能な内容となっている。

また、経済産業省の「情報システムの信頼性向上に関するガイドライン（以降、信頼性向上ガイドライン）」との関係は、信頼性向上ガイドラインが、情報システム利用者及び情報システム供給者を対象として、未然防止と事後対策の双方の観点から取りまとめられたものであるのに対して、本ガイドラインは、事故が発生することを前提として情報システム利用者における事後対策に重点を置き、より具体化したものとの位置づけであり、相互補完的なものとなる。

さらに、ISO/IEC 20000（情報技術－サービスマネジメント－）はサービスレベル管理の基準であるが、本ガイドラインを用いることで IT サービス継続性というサービスレベル管理について ISO/IEC 20000 のマネジメントシステムを活用することができる。

---

[1] 「組織」とは企業、行政、NPO 等も含む
[2] 情報システム部門、事務企画部門、バックオフィス部門など
[3] EUC（End User Computing）の担当者も含む

2. IT サービス継続

2.1 IT サービス継続とは

IT サービスは、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である。具体的には、財務会計システム、生産管理システム、在庫管理システム、顧客管理システムなどの基幹システムに加え、電子メールシステム、入館システム、スケジューラー、部門等で作成・提供されている表計算等の基幹システムではないシステムが提供する機能も IT サービスに含まれる。また IT サービスとは、組織内のユーザに対して提供される「サービス（機能）」に着目した概念であり、それがどのような「システム」により実現されるかは問わない。言い換えればその「サービス（機能）」が、企業等が自ら構築したシステムにより提供されるものなのか、外部のサービスプロバイダが提供するサービス（ASP 等）を利用したものであるかは考慮する必要はない（図 2.1-1）。

なお、近年、組み込み系システムの重要性が増してきているが、1）本ガイドラインの想定する対象者と組み込み系システムを提供している者が異なること、2）IT サービス継続のための対策が組み込みシステムの場合と異なることなどから、本ガイドラインにおいては、組み込み系システムを対象として取り上げないものとする。

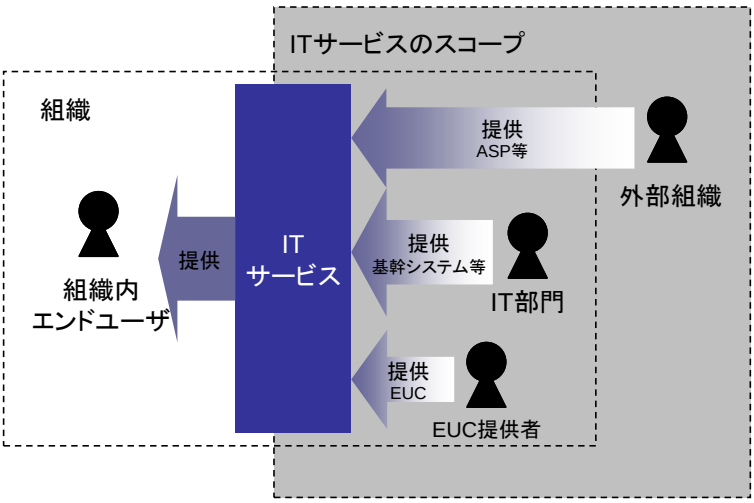

図 2.1-1　IT サービスのスコープ

IT サービス継続とは、事業継続の一部であり、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に応じて最適化するための取り組みである。IT サービス継続を実現するためには、IT に係る中長期の投資計画や体制面の整備が必要となるため、必然的に IT サービス継続は IT 戦略の一部ないし IT 戦略の次位に整合的に位置づ

けられるものである（図 2.1-2）。

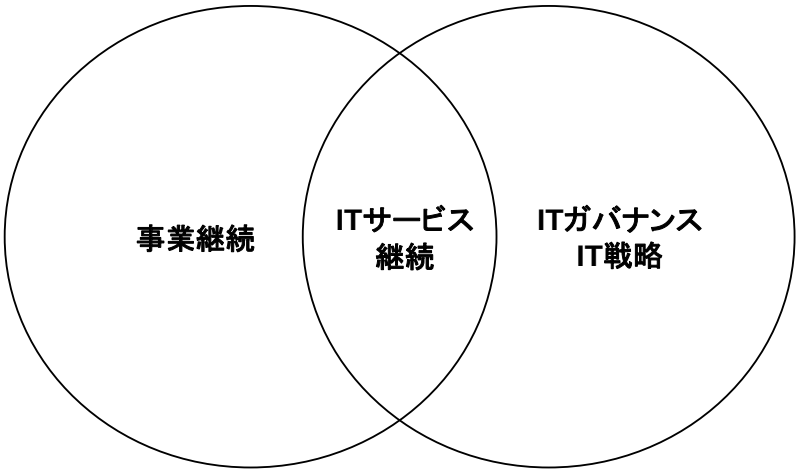

図 2.1-2　IT サービス継続、事業継続、IT 戦略との関係

情報セキュリティと IT サービス継続との関係については、以下のように整理される。情報セキュリティは、情報の機密性、完全性及び可用性を維持することとして一般的に定義されている[4]。これに従えば、IT サービス継続は、主に可用性の維持に関係するものとして位置づけることができる（図 2.1-3）[5]。実際には、情報セキュリティと IT サービス継続とは、どちらかが他方を包含する関係というよりも、相互に関係するものとして位置づけられる。そのため、経済産業省が定めている「情報セキュリティ管理基準」や JIS Q 27001 等の情報セキュリティに関する基準・規格等においても、事業継続計画（BCP）を関連要件の一つとしている。

[4] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security（2002）

[5] 広義の IT サービス継続には、機密性・完全性の要素も含まれ得るが、本ガイドラインでは主に可用性の面に着目し、情報の機密性と完全性の確保を主に情報セキュリティ上の責務と捉えた上で、IT サービス継続は常に情報セキュリティ対策と並行して確保すべきとの考えに立つものとする。

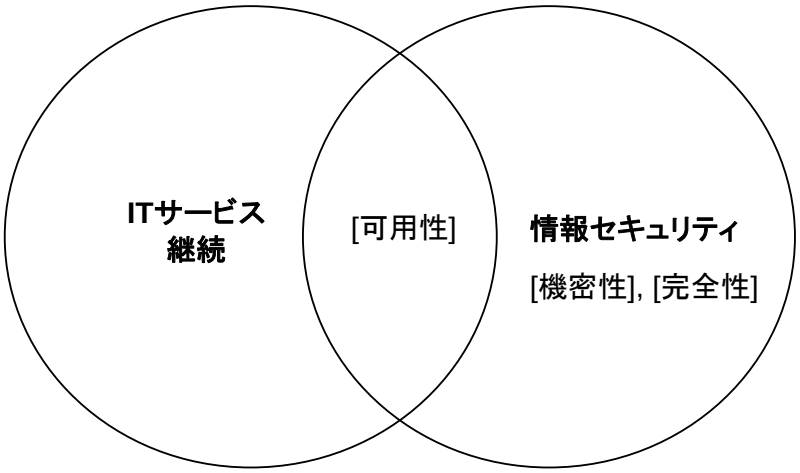

図 2.1-3　IT サービス継続と情報セキュリティとの関係

なお、緊急時においては、情報セキュリティのうち機密性と完全性の側面と IT サービス継続が主眼とする可用性の側面との両立が困難な場合も想定されるが、たとえば、企業の社会的責任や企業経営等の観点から、合理的な判断に基づきより重要と考えられる概念が優先される。また、全ての事態を事前に想定し計画を立てる事は非現実的であることから、権限委譲などによる現場における判断の余地を残しておく必要がある。

2.2　本ガイドラインの利用者

「IT サービス継続ガイドライン」は以下に示す 2 種類の利用者を想定している。

a）組織の経営層

組織の経営層は、組織の中長期的戦略、特に IT 戦略に基づき、IT が事業継続に与える影響の観点から組織が定めるべき中長期的目標及びリソースの配分等について検討を行い、IT サービス継続マネジメントを構築すると共に、IT サービス継続戦略を策定する必要がある。本ガイドラインの「4. IT サービス継続マネジメント」は、主に組織の経営層を対象としている。

b）IT 部門

IT 部門は、経営層が策定した IT サービス継続戦略に基づき、IT サービスの継続を技術的にどのように確保するか等について具体的な施策を策定する必要がある。本ガイドラインの「5. 管理項目」は、主に IT 部門を対象としている。

3. 定義

本ガイドラインで使用する用語を以下のように定義する。

a) IT サービス

IT サービスとは、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であり、その機能が組織外部により提供されるものであるか否かは問わない。

b) IT サービス継続

IT サービス継続とは、事業継続の一部であり、災害、事故等の発生に際し、IT サービスの中断・停止[6]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である。

c) IT サービス継続マネジメント

組織のマネジメントシステム全体の中で、事業リスクに対する取り組み方に基づいて、IT サービス継続の計画、実装、運用、維持及び監査に係る部分。

d) IT サービス継続戦略

組織の中長期的戦略の下に位置づけられ、IT が事業継続に与える影響の観点から組織が定めるべき中長期的目標、対策の方向性及びリソースの配分等を定めたもの。なお、ここでいう「組織の中長期的戦略」には、IT 戦略や、事業継続計画のうち経営戦略に係る部分等が含まれる。

e) 情報セキュリティ

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めても良い。

f) 事業継続マネジメント（BCM）と事業継続計画（BCP）

BCP・BCM は、事故や災害などが発生した際に、「どのように重要な事業・業務を継続させるか」もしくは「どのように重要な事業・業務を目標として設定した時間内に再開させるか」について様々な観点から対策を講じることである。BCP は、そのための計画自体を指し、BCM は、BCP の策定から運用、見直しまでのマネジメントシステム全体を指す。

---

[6] IT サービス継続が困難になるような機能低下も含む

g) 目標復旧時間（RTO)、目標復旧ポイント（RPO)、目標復旧レベル（RLO）

目標復旧時間（RTO：Recovery Time Objective)とは、事故後、業務を復旧させるまでの目標期間（時間）をいう。目標復旧ポイント（RPO：Recovery Point Objective)とは、事故後に事故前のどの時点までデータを復旧できるようにするかの目標時点（時間）をいう。目標復旧レベル（RLO：Recovery Level Objective)とは、事故後、業務をどのレベルまで復旧させるか、あるいは、どのレベルで継続させるかの指標をいう。

h) ディザスターリカバリープラン(DRP)、緊急時対応計画(コンティンジェンシープラン)、インシデント対応マニュアル、システム障害対応規程

ディザスターリカバリープラン（DRP)、緊急時対応計画（コンティンジェンシープラン）は、主に緊急事態（非常事態）が発生した場合の対応を規定するものであり、事前対策については含まれないのが一般的である。システム障害対応規程は、DRP 等の一部と考えられ、その対象は情報システムである。インシデント対応マニュアルとは、狭義には情報セキュリティ関連の事故に対応するためのマニュアルであり、システム障害対応規程とは対象がやや異なる。

4. IT サービス継続マネジメント

4.1　IT サービス継続マネジメントのフレームワーク

IT サービス継続マネジメントのフレームワークとは、事業継続マネジメント（BCM）の中から IT の要素を取り出して、そのマネジメント体制を事故前提の考え方で設計・実装・運用するための枠組みである。具体的には、

- IT サービス継続戦略(4.2)
- IT サービス継続計画(4.3)
- IT サービス継続体制の実装、運用、維持及び監査(4.4)

という個々のプロセスで管理される内容を全体としてマネジメントし、改善につなげる仕組み作り（PDCA）のモデルである（図 4.1-1）。

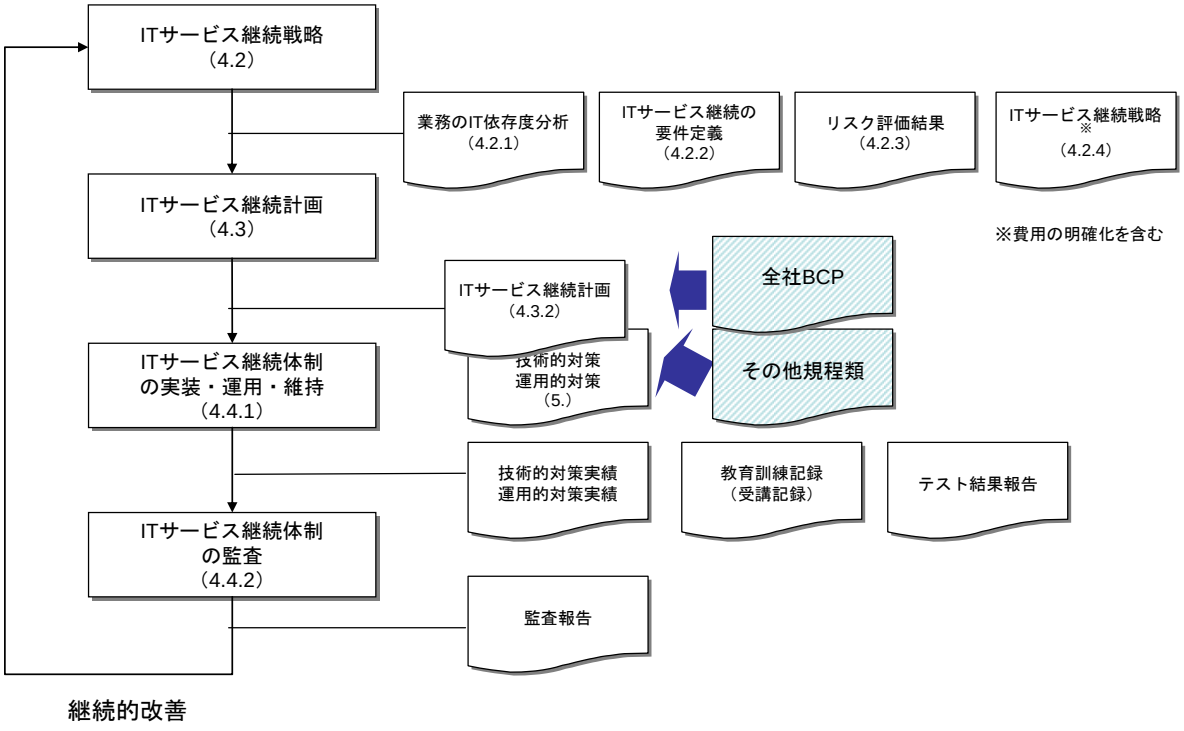

図 4.1-1　IT サービス継続マネジメントのフレームワーク

前述のように、IT サービス継続マネジメントは、事業継続マネジメントの中から IT の要

素を取り出したものであるので、全く新たな文書体系の構築を要請するものではなく、事業計画マネジメントへの取組みの中から作成してきた規程類のうち、IT に関わるものをサービス継続の観点で体系化するのに役立つ考え方である（BCP と IT サービス継続計画との連携例については、「参考 5」（P.17）を参照）。

4.2 IT サービス継続戦略

4.2.1 業務プロセスの IT 基盤への依存性

IT サービスは階層化されており、それぞれの IT サービスには全て依存するサービスやハードウェアがある（図 4.2-1）。これらについて、どのような依存性があるかについては、事故や災害の発生時などに調べるのは容易ではない。あらかじめ、IT の依存性や動作条件、設定条件について分析しておくことが必要である。また、IT サービスが停止した場合の業務に対する影響の分析（感応度分析）などを行うことが必要である。

事前に BCP が作成されており、維持すべき業務が決まっている場合は、その業務の IT への依存性について検討を行う。また BCP 策定時にビジネスインパクト分析（BIA：Business Impact Analysis）を実施している場合は、その結果を用いることができる。

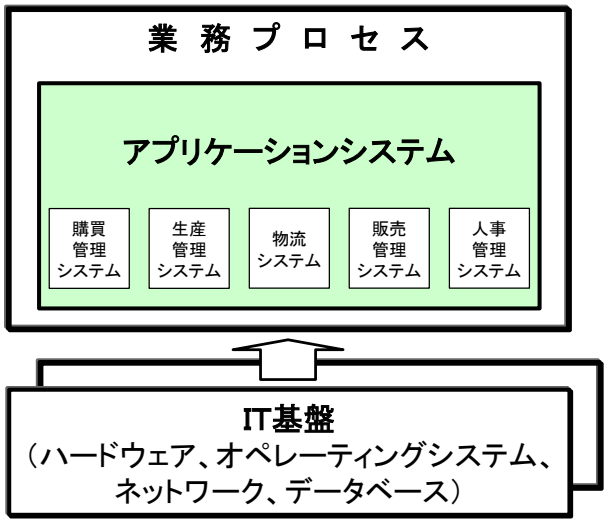

図 4.2-1 IT 基盤と業務プロセス

【参考 1: IT サービス継続と BCP】

組織として、既に BCP の作成を行っている場合は、BCP 作成のプロセスとして、ビジネスインパクト分析（BIA）が行われ、その結果として IT サービス継続の要件が定義されているはずである。しかし、JIPDEC（日本情報処理開発協会)が行った平成 17 年度の「情報セキュリティに関する調査」によれば､BCP を既に作成している企業は 16.5%で､作成中の 4.7%を考慮しても、残りの 79%の企業は BCP を作成していない。これらの企業では、IT サービス継続への投資決定を行うためには、まず初めに、経営者や業務部門も合意できる IT サービス継続の要件を設定する必要がある。

4.2.2 IT サービス継続の要件定義

(1) IT サービスの範囲

IT サービス継続の要件定義に際しては、「4.2.1 業務プロセスの IT 基盤への依存性」の分析結果を踏まえ、IT サービス継続マネジメントの範囲を決める必要がある。

具体的には、IT サービス継続を考慮するためには、組織が用いている IT サービスを洗い出すとともに、IT サービスの提供範囲やサービスレベルを明確にする必要がある。特に、IT 部門が組織の内部で、情報システムの企画から開発・運用までを担当しているような場合、業務部門からは IT サービスが何かわからないこともある。したがって、IT サービスについての分析を行う場合には、業務を行うために利用している IT が何かを明らかにする必要がある。特に、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について、事前に調査をして明確にしておく必要がある。さらに、これらの IT サービスが依存している基盤となる共通のサービス、例えば、組織のバックボーン LAN などについては特に配慮を行う必要がある。目的の IT サービスを提供する IT システムが稼動していても、ネットワークなどの基盤サービスが稼動していなければ、IT サービスも実質的に機能しない。すなわち、IT サービスの範囲を決める場合には、そのサービスが依存する基盤となる IT サービスも明確にしておく必要がある。

【参考 2： 共通な IT サービス】

多くの組織では、基幹システム以外にも、あらゆる場面で IT を活用している。電子メールやスケジュール管理はその一例である。その他にも、エレベータや入館システム、非接触型の認証カードなど､あらゆるものに IC チップが埋め込まれてコントロールされている。例えば、組織において電子メールの送受信ができなくなると、顧客との連絡が取れなくなること等を通じて、機会損失の発生等、業務への影響が生じる。また制御システムの故障によりエレベータが停止すると、高層ビルでは仕事ができなくなるおそれがある。このように、従来、IT が応用されていなかった分野でも、IT が停止すると組織活動に影響が出てくるものが多い。したがって、IT サービス継続を考える場合、このような共通の IT サービスも洗い出して、組織に与える影響を分析する必要がある。その際には、これらの IT サービスについても、その基盤となる IT サービスとの関係を明確にしておく必要がある。

【参考 3： 業務の IT サービスへの依存度】

目標復旧時間の短い重要な業務において、IT サービスの復旧が長引いても、手作業などによる代替手段が存在することで、一定の期間内において、ある程度のレベルで業務を継続できる場合がある。したがって、IT サービスの範囲を検討する際には、業務の IT サービスへの依存度を予め明確化しておく必要がある。目標復旧時間が短く、IT サービスの停止が即業務停止につながる業務が、IT サービス継続に対する要件が最も厳しいものとなる。

⑵ 要件定義

IT サービスの継続を考える上では、IT サービスの中断・停止につながる事象が発生した場合、その IT サービスを復旧させる活動の目標を設定することが重要である。この際に用いる指標は、一般に RTO、RPO、RLO の 3 項目からなる。これらを適切に設定することは、IT サービス継続戦略を策定する際に、経営者、業務部門、IT 部門、社外の取引先といった関係者間での共通理解を醸成する上で重要であり、IT サービス継続マネジメントを行う基本的な要件となる。その一方で、コスト面も含めた最適化を行う必要がある。IT サービスを利用する部門に対して、コスト面での制約を与えずに、IT サービス継続の要件定義をさせれば、RTO と RPO がゼロで、RLO は事象の発生前と同等という要件が当然の結果として出てくる。しかし、こういった要件を満足させるためには、コスト的にも非常に大きな負担が必要になる。したがって現実には、開発要員数等も含めた広い意味でのコストと、その IT サービスを利用している業務に対する影響度を勘案して、要件定義を行うべきである。

なお､要件定義に際しては､BCM において定められた要件への適合を確認することに加え、組織の IT 戦略等との整合性についても確認する必要がある。なお、要件定義に際しては、

BCM において定められた要件への適合を確認することに加え、IT サービスとして外部サービスを利用している（利用しようとする）場合も、IT サービスに与える影響を、IT サービス継続、情報セキュリティ、費用対効果等の観点から幅広く検討する必要がある。

なお、要件定義と情報セキュリティの関係については、「4.3.3　緊急時におけるセキュリティ水準の低下」を参照のこと。

【参考 4： 業務の目標復旧時間（RTO）】

IT サービス継続において最も優先する要件は、IT サービスが支える組織における業務の目標復旧時間(RTO)である。組織において BCP 等が策定されており、RTO が明らかな場合には、業務を支える IT サービスの範囲を構成管理情報などを用いて明確化し、業務を RTO 以内に復旧させることが IT サービス継続の要件となる。ほとんどの場合、IT サービスは業務再開の前提条件となるため、IT サービスの復旧を RTO より短い時間で行うことが要求される。組織において RTO が明確でない場合には、業務部門と情報システム部門との間で、RTO に関する意識合わせを事前に行う必要がある。

RTO は、業務停止によるビジネス全体への影響度により決定される。顧客への影響が多い受発注業務や出荷指示、問い合わせ対応のコールセンター業務などが優先的に復旧すべき業務とされる場合が多いが、コミュニケーションのインフラとしての電子メールシステムや、全社イントラネットなども停止時の影響範囲は大きく、復旧優先順位は極めて高い。

要件定義のためのアプローチとしては、以下の二つが考えられる。

まず、各業務プロセスからのアプローチとして、その業務の中断・停止が経営に与える影響を分析し、その大きさからその業務で使用している各 IT サービスの継続要件を求める方法がある。このアプローチのメリットは、1) 業務プロセスの中断・停止という経営者や事業部門にわかりやすい領域から始めること、2) その業務プロセスの責任者自身が業務の中断・停止が経営に与える影響を分析することから、最終結果について経営者や事業部門の納得を得やすいことが挙げられる。なお、このアプローチにおいては、広い範囲の IT サービスについて検討するためには、経営者のリーダーシップのもとに、組織内の広い範囲の組織を参加させて検討を行う必要があり、事前に経営者の理解を得る等の条件を満たす必要があることに留意する必要がある。外部の規制を受ける機関（例：金融機関等）では、コンプライアンス達成のためと言う理由でこの条件を満たすことができる可能性も高いが、それ以外の組織ではこの点が難関になると見られる。

もう一つのアプローチは、IT サービスの中断・停止を引き起こすリスクが現実となった時に想定される事態をまとめ、IT サービスの中断・停止が各業務プロセスに与える影響を分析し、さらに、その業務の中断・停止が経営に与える影響の大きさから、その業務で使用している各 IT サービスの継続要件を求めるアプローチである。このアプローチのメリットは、BCP が策定されていない状況下で、IT 部門が主導して IT サービスの継続要件をまと

める場合には、事業部門の作業負荷が少ないことから、要件定義を開始することが容易となる点である。一方、このアプローチにおいては、全てを IT だけで解決しようとする方向に陥ることで、業務部門が手作業のバックアップ手段を取れば簡単に対応できる作業を洗い出すことができなくなるなど、結果として、全ての IT サービスに高い継続要件が求められることになりかねない点に留意する必要がある。

4.2.3 リスクの評価

本項では、IT サービスを支える情報システムに内在するリスクを整理し、IT サービス継続計画が組織全体での事業継続計画と連携するためのポイント、及び IT サービス継続において想定すべきリスクとその評価について述べる。

(1) 事業継続とシステムリスク

IT サービス継続計画を検討するに際しては、情報システムの持つ特徴を無視することはできない。

図 4.2-2 は、情報システムが各種のインフラによって支えられていると共に、ネットワークの発展により利用者が広域にわたっていることを示している。

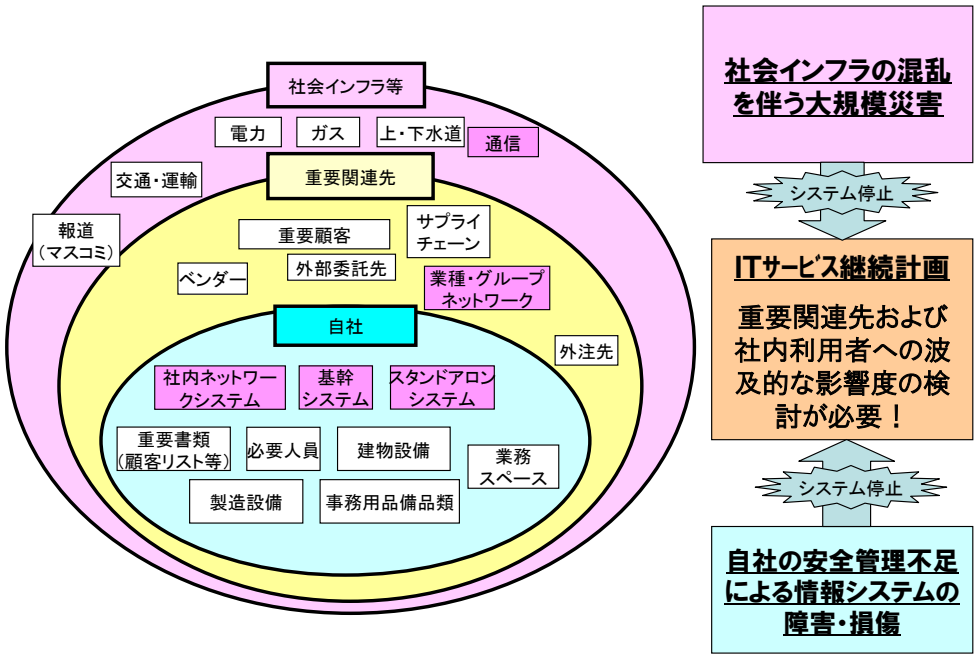

図 4.2-2 情報システムを取り巻く社会環境と IT サービス継続計画

IT サービスは、それを提供しているハードウェアが存在している場所（マシンルーム等）の周辺に留まらず、日本全国、場合によっては全世界へ広がっていることも少なくない。

地震など地域全体に大きな被害を生じる事象が発生した場合には、情報システムも生産設備と同じく、電力の途絶などによって影響を受ける。

しかし、情報システムは、他の生産設備と異なり、バックアップ設備を他の場所に設置する等の措置を通じて事前対策を比較的容易に行える設備のひとつである。あるシステムの中断・停止が大きな影響を与えうるにもかかわらず、組織が必要な対策を講じていなかった場合は、その組織は本来であれば回避可能であった損失を蒙る危険性がある。

加えて、IT サービスの継続が阻害されることは、自組織のみならず、顧客等のステークホルダーに対しても大きな影響をもたらすおそれがある。

これは、IT サービス継続計画の検討に際しては、全組織における BCP で想定する地震等の大きなリスクと比べて相対的に局所的・小規模である、マシンルームの火災等のようなリスクについても考慮する必要があることを示している。

具体的なリスク評価のプロセスは以下の通りである。

① 「リスク（リスクの原因事象）[7] 」の洗い出し

計画の策定に先立ち、どのようなリスクがあるかを洗い出すことが必要である。

この際には、ある特定のリスクに限定せず、まず組織に想定されるリスクをできるだけ洗い出すことが重要となる（表 4.2-1）。その上で、この中から情報システムに関連するリスクを絞り込んでいく。

また、リスクは組織内外の業務内容や環境の変化、情報システムの利活用状況の変化によって絶えず変化するため、定期的な見直し作業も必要となる。

[7] リスクの原因事象が発生することによって、組織の経営等に与える影響を結果事象と呼ぶ。

表 4.2-1　組織を取り巻くリスクの原因事象の事例（金融機関の例）

主要因	分類	想定リスク（原因事象）
システム的要因	安全・環境	自然災害
		設備事故・破壊・過失
		社会的インフラの障害
		公害・エネルギー問題
		リサイクル問題
		大規模感染症の流行　等
	情報管理	情報漏洩
		情報遮断　等
	犯罪	コンピュータ犯罪
		カード犯罪　等
	社会的責任	金融機能停止・遅延
	商品・サービス	提供停止・遅延
社会的要因	法務	施設立地訴訟
		知的財産権訴訟
		独占禁止法違反　等
	人事・組織	雇用差別
		労働災害
		人材の確保問題
		内部告発　等
	社会的関連	不正確・不適切な情報開示（ディスクロージャー）
		不適切・非活発的な地域振興活動
		従来慣行の問題化
		事務ミス・事故
		不祥事
		文化摩擦　等
損失	財政的損失	設備損害
		供給停止
		補償
		労務対策費　等
	人的損失	企業内死傷者
		第三者死傷者
		追加業務発生　等
	社会的信用損失	一般公衆、地域住民、監督官庁からの信用低下
		従業員の意欲低下
		顧客トラブル
		資金調達力低下　等
	その他	テロ行為

（三菱総合研究所編「リスクマネジメントガイド」をもとに作成）

② システムリスクの想定

システムリスクに関するものとして、以下のような事象が想定できる（表 4.2-2）。

表 4.2-2　システムリスクに関する分類の例（金融機関の例）

分類	想定されるシステムリスク		
自機関（外部委託を含む）の内部に起因する障害	故障	ハード関連	ハードウェアの故障
			処理能力オーバーフロー（ハードウェア）
		ソフト関連	処理能力オーバーフロー（ソフトウェア）
			ソフトウェアの故障
	過失		オペレーションミス
			その他の過失（不十分な管理による機密情報漏洩等）
自機関の外部に起因する障害	故障		通信回線関連の故障
			停電
			外部コンピュータシステムの故障
	広域災害		自然災害および火災
	局所災害		自然災害および火災
コンピュータ犯罪			コンピュータ本体または付帯設備の破壊
			電磁的記録物の破壊
			データまたはプログラムの改ざん・消去（不正アクセスまたはコンピュータウィルスも含む）
			ハードウェアの不正使用（不正アクセスを含む）
			データまたはプログラムの不正入手
			不正データ入力
カード犯罪			キャッシュカードまたはクレジットカード犯罪

（注）金融機関の場合、自機関には、外部委託先も含むため、外部委託先の障害は「内部に起因する障害」とみる。[FISC.1]

【参考 5： BCP と IT サービス継続計画】

組織全体での BCP（全社 BCP）に関する取り組みでは、想定する事象として、地震などの大規模災害が取り上げられる場合が多い。一方、情報システムに関しては、大規模災害のみならず、システム本体及びインフラ[8]における事故などによっても、多数の利用者が影響を受ける。このため、IT サービス継続計画の策定に際しては、より局所的・小規模なリスクに対しても配慮する必要がある。

ただし、不正アクセスや操作ミス、情報漏洩事故など、情報セキュリティで取り扱うすべてのリスクを対象とすると、実施すべき対策の範囲が広がり過ぎるおそれがある。

地震などを想定した全社 BCP と連携した IT サービス継続計画を策定する場合には、システム本体及びインフラの損傷や途絶などに絞り込み、不正アクセスなどのリスクは別プロジェクトで検討することも選択肢の一つである。

実務的には、全社 BCP の対象となる活動やリスクを十分に理解し、全社 BCP と連携しながら、IT サービス継続計画において想定すべきリスクを検討することが必要となる。

全社 BCP と IT サービス継続計画との連携例としては、図 4.2-3 のようなフローが考えられる。

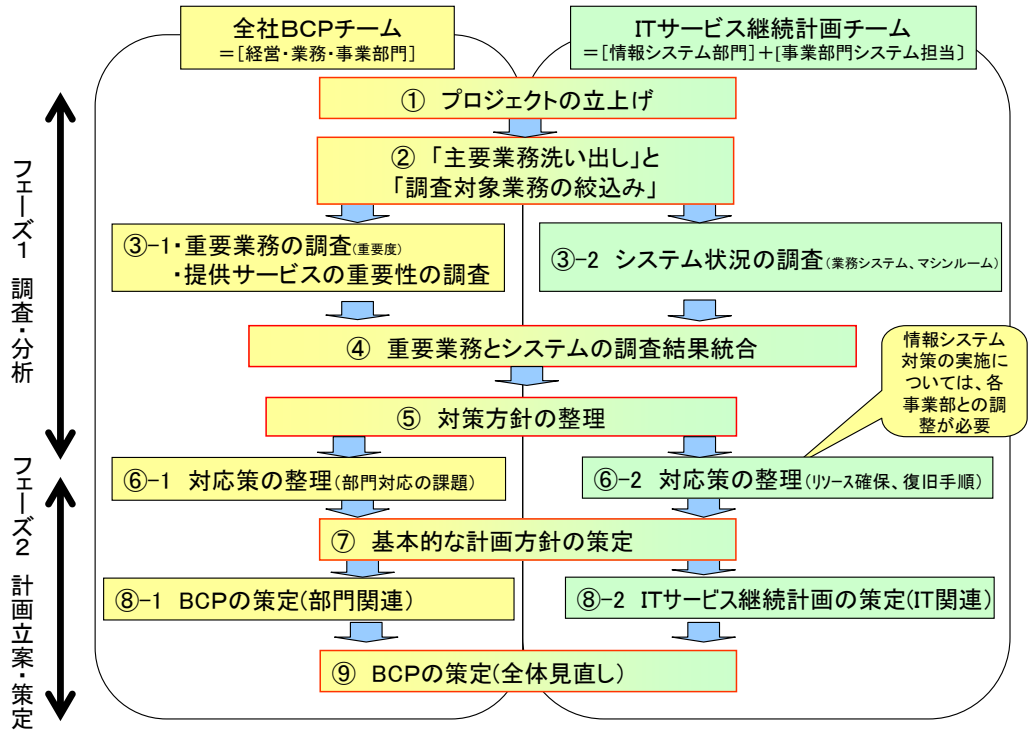

図 4.2-3 全社 BCP＆IT サービス継続計画の連携例

[8] 例としては、電力・通信回線・上下水道が挙げられる。

また、目標復旧時間（RTO）については、通常業務において情報システムに求められる目標復旧時間を短時間としている場合、全社 BCP で想定される状況下で求められる復旧時間とは、大きく乖離することが多い。これは、全社 BCP では、インフラを含む様々なリソースへの甚大な被害など、社内外の広範囲にわたる影響を想定した上で、サポートの遅れやリソースの確保などの要因を考慮しなければならないことから、目標復旧時間が長くなるためである。

このように、IT サービス継続計画チームの中では、通常業務の中で想定されるリスクと、全社 BCP で想定される非日常的なリスクを区別して議論することも必要である。このためには、全社 BCP で想定されるリスクを表 4.2-3 の様に整理し、IT サービス継続計画チームの意識を切り替えることも重要である。

また、電子メールや IP 化された内線電話などの通信手段の早期復旧が、全社 BCP の目標復旧時間を実現するための前提となることも少なくない。このような IT サービスについては、全社 BCP で定められた利用計画を踏まえ、復旧する範囲や目標復旧時間を設定することが重要である。

表 4.2-3　IT サービス継続計画で想定すべきリスク例

※全社 BCP で想定されるリスクに対して、IT サービス継続計画の特徴を考え、想定するリスクの原因事象と結果事象の組み合わせを整理。

ケース	規模	範囲	想定リスク（原因事象）	想定される被害（結果事象）
A	大	広域	大地震	・インフラの長期停止 ・IT 設備の損壊 ・復旧要員の不足 ・復旧活動拠点の喪失 ・建物内への立入り制限
B	中	局所 （内部）	火災、…	・インフラの被害なし ・サーバ室、データ室単位でのシステム機器の損壊
C	小	局所 （外部）	インフラ事業者の事故、…	・インフラの短期停止 ・システム設備の被害なし
…	…	…	…	…

※損壊とは、再調達が必要な状態。

(2) IT サービス継続において想定すべきリスクの影響・結果

IT サービス継続において想定すべきリスクの影響・結果は、IT サービスの提供が中断したり停止することによりもたらされる事態の発生である。ここでは、中断・停止を、その期間により比較的短期的なものである中断と、中長期的なものである停止とに区分する。ただし、長短について一律に特定することは適切ではなく、個々の組織の環境、業態等により個別に判断されるべきである。

上記を受け、IT サービス継続の想定すべきリスクの影響・結果は下記のようになる。

- 目的業務の運用の中断・停止
- 目的情報の入手の中断・停止
- 目的情報の提供の中断・停止

IT サービスの中断が復旧せず、停止に至る場合がある。

また、IT サービスの中断・停止が、局所的である場合と、広域に及ぶ場合がある。一次的局所的中断により、二次的、三次的な局所的中断が生じ、それが広域化した中断となり、ついには広域での停止に至ることもある。このような事象の防止のために、一次的局所的中断時に、敢えて局所的停止を宣言、採用し、その広域化を回避する施策が有効な事態も経験されるところである。

(3) IT サービス継続の阻害要因

IT サービス継続に対する阻害要因については、従来から多くの研究、検討がなされており、下記のようなものが挙げられている。

- システム環境・基盤の不備・不全
- ハードウェアの不備・不全
- ネットワークの不備・不全
- ソフトウェアの不備・不全
- データの欠陥・不適合
- 要員の不足・能力低下

建物設備、電力、水道、空調等のシステム環境・基盤において、その損壊、停電、断水等の整備・運用の不調、機能不全は、IT サービスの継続の阻害をもたらす。ハードウェア、ネットワーク、ソフトウェアの不調、機能不全も同様である。IT サービスの目的を実現するためのデータが不完全、不適合により、システムが影響を受け IT サービス継続が阻害される場合がある。IT 施設への往路の途絶等で稼動要員が不足したり、要員不足による操作

能力水準に至らないなどは同じく IT サービス継続が阻害されることになる。
　これらの阻害要因の背景には、大きく人為的意図的なものと、その他の非意図的なものとがあり、それぞれ次のように分類される。

＜意図的要因＞
・故意による人の行動

＜非意図的要因＞
・自然現象
・物理的・化学的現象
・過失による人の行動

　上記において、故意による人の行動には、悪意に基づくテロ、暴動、破壊活動のほか、先述した局所的中断の広域化を回避するために緊急避難的に実施する行動も含まれる。
自然現象は、風水害、雷、地震等である。物理的・化学的現象には、風化、材質疲労、材質劣化・変質等が含まれる。
　過失による人の行動は、個性、見識不足、精神的疲労、肉体的疲労等によりもたらされる手続ミス、操作ミスなどである。
　上記の各事象は、先述の IT サービス継続のそれぞれの阻害要因のすべての原因となりうるものである。
　原因の発生を防止できれば、阻害要因は生じないが、原因の防止については、人の行動のように統制可能なものと、自然現象のように統制不能なものがある。
　統制可能な阻害要因に対しては統制を検討し防止、低減を図るべきであるが、統制不能な阻害要因については統制以外の管理を検討しなければならない。

⑷ リスクの評価手法
　IT サービス継続計画は、想定すべきリスクの評価に基づき策定される。リスク評価結果は、計画策定に当たり、個々の計画適用の手順、詳細度、適用の多重化等に影響する。
　IT サービス継続計画についてリスク発生に対応する局面を重視すれば、リスク評価はリスクの阻害要因の分類を中心に実施すべきである。IT サービス継続計画についてリスク防止の観点を加味する場合は、リスク評価はリスクの原因の分類を基準として検討すべきである。
　リスク評価は、上述した IT サービス継続の阻害要因及び原因の分類等に基づく個々のリスクについての評価結果を、相対的あるいは絶対的な水準として求めるべきものであるが、その評価手法については、先行した研究・実践が参考となる。本報告では、定量評価、定性評価に関して、それらの紹介にとどめ詳細な適用形態については別途の検討としたい。

例えば、下記のようなものが適用可能である。

＜定量評価法の例＞
- コートニィ理論:「頻度×大きさ」によりリスクを計算評価
- GMITS 方式:「資産価値×脅威×脆弱性」によりリスクを計算評価
- 米国 NIST 方式:「頻度×損失」によりリスクを計算評価

＜定性評価のための考慮軸＞
- 代替手段、代替情報の利用の可否
- 業務諸環境の相対的重要性
- IT の成熟度、浸透度
- 経営目標、情報戦略

4.2.4 戦略策定

「4.2.2 IT サービス継続の要件定義」では IT サービスについての要件定義を明らかにした。次に重要なのは、リストアップされた IT サービスについての優先度を明確にすることである。

まず、組織にとっての BCP や BCM を参考にして、優先すべき業務を洗い出す。特に、事業継続に不可欠な部分を占める業務（例えば、企業の収益の重要な割合を占める業務）が IT に全般的に依存している場合には、該当する IT サービスの重要度が高いといえよう。一方、組織にとって、他の手段で業務を維持できるものについては、IT サービスの重要度は低い。ここで留意すべきなのは、共通の IT サービスと基盤の IT サービスについても検討することである。これらは、事業に直接関係しないため、その重要度を見誤る危険性が高い。例えば、電子メールが使えない時や、停電により入館システムが動作せずオフィスに入館できない時の影響を検討する必要がある。また、生産管理システムなどの基幹システムが動作していても、ネットワーク等の共通の IT サービスが動作していないと、基幹システムに必要なデータが提供されず、結果として IT サービスが機能しないことがある（詳細は「4.2.2 IT サービス継続の要件定義」を参照)。IT サービス継続戦略には、これらの検討結果を記載することが重要である。

BCP や BCM において、組織の重要な事業についての戦略策定がなされていても、本来必要なこれらの共通の IT サービスや基盤の IT サービスについての検討が不十分である場合も多い。IT サービス継続戦略策定にあたっては、事業の観点から作成された BCP や BCM と IT サービス継続との関係をマッピングする必要がある。IT サービス継続戦略の対象となる IT サービスを一覧表形式で洗い出した上で、関係する業務の重要度を記入し、優先度を明確にする。次に、それらの IT サービスが依存する IT サービスを明確にして、それらの IT サービスの優先度も見直す（詳細は「4.2.2 IT サービス継続の要件定義」を参照)。IT サー

ビス継続戦略には、IT サービスの優先度等を記載することが重要である。

IT サービスとそのサービス継続に向けた優先度が決まれば、そのリストを基にして、必要な IT のリソース（ソフトウェア、ハードウェア）を明確にする。さらに、IT リソースを調達するためのコストを明確にした上で、これらのコストと、IT 戦略や BCP・BCM で想定している予算との調整を行う。また近年では、複数の業種において、コストの削減等を目的として、システムの相互バックアップやデータセンターの共用化など、他の組織（同業他社等）と BCM に関する共助体制を事前に構築した例も存在する。

なお、IT サービスの場合、国や規制機関からの要請によって、優先度を変更しなければならないこともある。特に、重要インフラと位置づけられた組織では、国や地方自治体の防災計画等との整合性などに配慮する必要がある。

戦略策定にあたっては、IT サービスの「計画（企画）」、「実装（取得・導入）」、「運用」、「維持」、「監査」というマネジメントプロセスにおいて、IT サービスの継続について考慮する必要がある。特に、情報システムの導入や変更を実施する場合には、IT サービスを継続する視点を入れたマネジメントプロセスの導入が望まれる。

【参考 6： 戦略策定実施例】

1) IT サービス継続要件と構成情報の整理
   自社の重要業務の許容中断時間の把握と該当業務を支える IT サービスの構成（業務を支えるアプリケーション・ハードウェア・ネットワーク・設置環境・運用要員などの構成管理情報）の明確化。
2) リスク評価
   IT サービスを取り巻くリスクの洗い出しと検討対象リスクの決定。
   検討対象リスクに対する現状の脆弱性の洗い出し（バックアップシステム有無、データバックアップ状況、データセンター耐震化状況、ネットワーク二重化、UPS 設置状況など）。
3) IT サービス継続戦略の検討
   自社の重要業務を許容中断時間以内に復旧させるための、IT サービスの継続戦略案（現状システムの修理・再調達による復旧、バックアップシステムへの切替などの代替手段による復旧等）の検討と、現状の IT サービスの脆弱性を踏まえた戦略実現に必要な対策（技術面・運用面）にかかる費用の明確化。
4) IT サービス継続戦略及び対策の決定
   各戦略の費用対効果（対策に必要な費用と要件の達成度）を踏まえ、採用すべき戦略を決定し、戦略を実現するために必要な対策と必要な投資を組織として意思決定する。

4.3 IT サービス継続計画

IT サービス継続計画は、IT サービス継続戦略により定められたサービス継続のための要件（組織にとって重要な IT サービスの明確化及び目標とすべき復旧時間・レベル）を踏まえ、これを実現するために必要な、事前の対策及び緊急事態発生時における具体的な対応方法・計画等を取りまとめたものである。

4.3.1 計画（文書）の策定

IT サービス継続の能力向上に向け、平常時において実施すべき対策の詳細と実施及び運用改善方法を定めた事前対策計画と、緊急事態が発生した場合の対応方法を定めた事後対応計画を策定する。

(1) 事前対策計画

バックアップシステムの構築や、データのバックアップの実施、サーバルームや情報システムセンターの耐震強化などの物理的な対策を定めた対策実施計画に加え、緊急時の対応能力の向上や、IT サービス担当者の意識向上を目的とした教育訓練計画、さらには IT サービス継続性の継続的な維持改善を行うための管理方法を定めた維持改善計画を策定する。

(2) 事後対応計画

緊急事態が発生した場合に IT サービス中断・停止が組織の業務に深刻な影響を与えないうちに復旧再開するための、対応体制・プロセス・対応手順を事後対応計画（緊急時対応計画）として策定する。

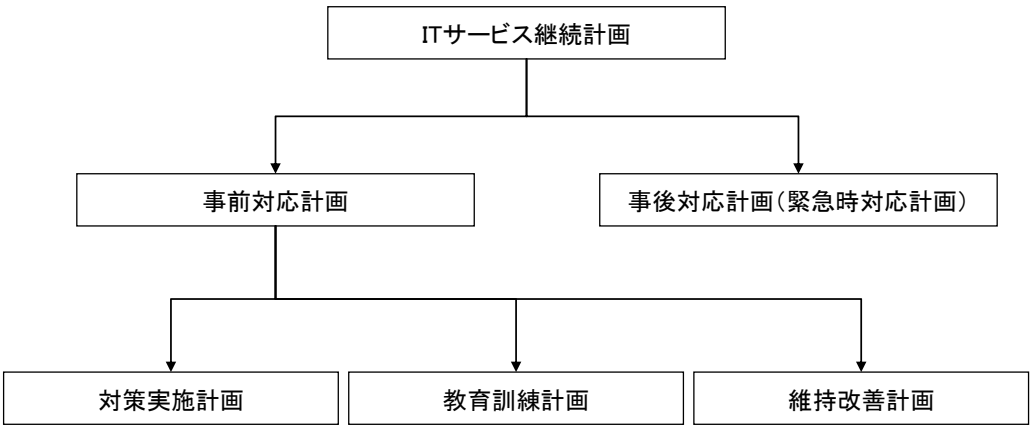

図 4.3-1 IT サービス継続計画の構造

4.3.2 計画に記載される項目

(1) 対策実施計画

「4.2 IT サービス継続戦略」において定められた戦略を実現するための具体的な対策内容を決定し、組織の行動計画として経営者の承認を得る。

【記載項目例】

a) IT サービスの継続要件

b) 実現方法

- 技術的対策：採用するバックアップテクノロジーの決定、システム構成、ネットワーク構成など
- 運用的対策：バックアップ運用手順の決定など

c) 実施スケジュール

d) 必要な投資

(2) 教育訓練計画

IT サービス継続計画を組織内に定着化し、緊急時における対応能力の向上につなげるための教育訓練計画を定める。「気づき」を得るための全体教育から、情報システムの切り替えテスト、業務担当者を含めた総合演習など、対象者と目的ごとに様々な手法を組み合わせ実施する。

【記載項目例】

a) 教育訓練の目的

b) 教育訓練の対象者と達成目標

部門責任者・全 IT 担当者・役割別担当などの対象者の範囲と対象者ごとの目的（「気づき」、習熟度向上、問題点の発見など）を明確化し、達成目標（評価指標）を決定する。

c) 教育カリキュラムと実施スケジュール

d) 評価と改善へのフィードバック

(3) 維持改善計画

IT サービス継続性の継続的な改善に向けた管理プロセスを明確化し、維持改善計画として定める。

【記載項目例】

a) 維持改善の目的

b) 維持改善の体制

c) 維持改善方法（点検時期、点検項目、点検主体）

d) 実施スケジュール

e) 改善へのフィードバック

(4) 事後対応計画（緊急時対応計画）

緊急事態発生時における情報システムの迅速な復旧・再開に向けた体制及び対応方法を定める。

【記載項目例】

a) 緊急時対応体制

緊急事態に設置する対策本部の役割と機能、対策本部員の連絡方法と連絡先などを記載。対策本部長などの重要な役割を担う要員については、代替要員（及び順位）をあらかじめ決めておく。

対策本部内の担当チーム例：

設備インフラ担当・ネットワーク担当・システムインフラ担当・アプリケーション担当・渉外担当・外部ベンダー連絡担当・ロジスティクス担当など。

b) 緊急時対応プロセス

緊急事態における対応プロセスの全体を定める。特に緊急事態発生時におけるバックアップシステムへの切り替えなどの IT サービス継続計画発動基準及び発動者の決定が重要。

対応プロセス例：

① 初動プロセス（問題の検知から通報～対策本部設置～被害評価～IT サービス継続計画発動）
② 復旧再開プロセス（IT サービス継続計画発動～再開）
③ 代替運用プロセス（バックアップサイトなどの代替手段による運用）
④ 完全復旧プロセス（機能完全復旧～代替手段からの切り戻し）

c) 緊急時対応手順

担当チーム毎の各プロセスにおける対応手順の詳細を定める。

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
- ネットワークリカバリ手順書
- 情報システム復旧手順書
- 対応項目チェックリストなど

4.3.3 緊急時におけるセキュリティ水準の低下

組織において求められる情報セキュリティ水準は、情報セキュリティに関係するリスク分析に基づいて、その組織が受容できないと判断するリスクに対して、そのリスクを軽減・分散・転嫁等するための管理策として決定される。

そのため、リスク分析では、組織として平常時における一定の水準を定めることになるが、緊急時においては平常時と異なる水準を認めざるを得ない場合も考えられる。言い換えると、平常時では受容できないとしていたリスクの一部を、緊急時にのみ受容する場合があるということである。具体的には、情報セキュリティ水準のうち、可用性の水準を維持するために、機密性及び完全性に関する水準の低下を認める場合がある。ここでいう緊急時とは、IT サービスの継続が困難となる事態であるが、あらかじめ分析して定めたリスク管理策の維持と IT サービス継続が相反する場合に、そこで改めて IT サービス継続が中断するリスクを加味した上で、可用性以外の情報セキュリティ水準を決定する必要がある。

ISO/IEC 18044:Information Security Incident Management では、「計画準備段階として事前計画に基づく対応手順を充実させて、実際のインシデント発生時に、手順にしたがって対応することを基本としている。しかし、その一方で、計画準備段階に用意した手順がインシデントの実情に沿わないときには、手順以外の方法による対応をするための手続きも必要であること」を指摘している。なぜなら、インシデント発生時においては、事前予測の想定範囲外の状況となることもあり、その場合には、事後対応を事前計画で想定した範囲内だけで実施することは、むしろ想定外の状況に柔軟に対応できなくなる場合があるためである。そのため、想定外の状況に遭遇した場合に、実際の担当者が事前に定められた処置よりも適切であると判断する処置を、例外処置として実施するための手続きを事前に検討しておくことも必要である。ISMS ユーザーガイド第 2 版[JIPDEC.1]では、そのような例外処置についても管理するような管理策を講じることについて述べている。このことから、緊急時における情報セキュリティ対策の不実施による情報セキュリティ水準の低下に加え、想定外の事態において IT サービス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情報セキュリティ水準の低下についても検証しておくことが重要である。

4.4 IT サービス継続体制の実装、運用、維持及び監査

4.4.1 実装、運用及び維持

IT サービス継続計画を策定し体制を構築した後は、その実装、運用及び維持を行う必要がある。具体的な実装方法（管理項目）に関しては「5. 管理項目」に示す。

IT サービス継続計画の実装に際しては、以下のような点を考慮する必要がある。

- 他の規程・計画（BCP を含む）との整合性
- 外部サービスの活用の是非
- 稼動テストの方法

また、IT サービス継続体制の運用及び維持に際しては、以下のような点について検討する必要がある。

- 教育、周知、訓練
- 自主点検

4.4.2 監査

IT サービス継続計画の監査は、リスクマネジメントの一環として及びリスクマネジメント全体の評価の観点を踏まえ実施される。IT サービス継続計画も PDCA サイクルにしたがって管理されるべきであり、

a) 計画の策定
b) 計画の導入・訓練
c) 実施・訓練状況の評価
d) そのフィードバック改善等

のフェーズが遂行されることになる。このリスクマネジメントのサイクルの中で、c)の評価がリスクマネジメントの一環としての「運用的対策としての監査」であり、また a)から d)までの過程全体を評価するものが「リスクマネジメント全体の評価としての監査」である。

運用的対策としての監査は主に、IT サービス継続計画が周知徹底され、個々の対策がそのとおり運用されているかという、いわゆる準拠性の監査として実施される。

リスクマネジメント全体の評価としての監査は、IT サービス継続計画のリスクマネジメントサイクル全体について、リスク分析を基礎として、個々の対策を含めて計画それ自体の妥当性、マネジメント運営の適切性を、総体として評価するものであり、準拠性はその観点の一部である。

組織を社会的存在として捉え、IT サービス継続もひとつの社会的責任の遂行とする観点からは、一定の社会規範たる IT サービス継続計画に係る規準に基づく外部監査の実施を検討する必要がある。

5. 管理項目

5.1 IT への依存性の検討

「5. 管理項目」の検討においては、「4. IT サービス継続マネジメント」を通じて行った業務の IT への依存性に関する分析の結果を、システム化の観点からより詳細に検討していくことになる。

具体的には、IT サービスの階層化は、選択する技術やシステムの構成につながり、IT サービス継続の要件定義を詳細に検討していくことは、さらに具体的な製品やその構成、コストの再評価をすることにつながる。

さらには、そうして検討された項目が実際にシステム化され、運用段階になった場合に、どのような基準で運用していくのかを検討することで、実効性のある IT サービス継続計画にしていく必要がある。

5.2 システムアーキテクチャの検討

「4. IT サービス継続マネジメント」を通じて決定した IT サービス継続の要件、戦略（重要な IT サービスの明確化及び目標とすべき復旧時間・レベル（RTO、RPO、RLO））を踏まえて、これらを実現するために必要となる技術的対策を決定することが必要である。この技術的対策を踏まえて IT サービス継続計画を策定する。

(1) システムアーキテクチャの検討

技術的対策の決定においては、まず、対象とする IT サービスに対して目標とする RTO、RPO、RLO、すなわち、目標とする IT サービス継続のレベルをどのようなシステムアーキテクチャで実現するかを検討する。システムアーキテクチャの例を図 5.2-1 に示す。また、検討の前段階として、現状の IT システム構成を整理し、目標とする IT サービス継続レベルの達成という観点から評価することが必要である。

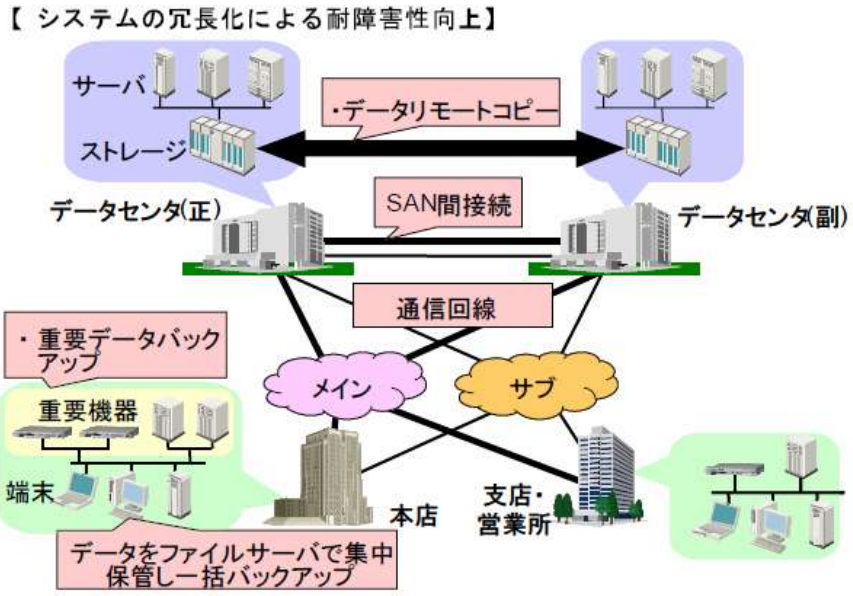

図 5.2-1　システムアーキテクチャ例

（出典：経済産業省「事業継続計画（BCP）策定ガイドライン」[METI.1]）

(2) 費用対効果の検討

この検討においては、コスト面での制約についての評価が重要である。一般的に、RTO、RPO を短く、RLO を高くしすぎると、必要となるコストが膨大になる可能性があり、技術的対策に要するコストと IT サービスの中断・停止による損失とのバランスを取ることが重要である。なお、コスト面については IT サービス継続の要件定義及び戦略策定時に検討・決定されているものであるが、具体的なシステムアーキテクチャの検討段階において、より具体的な実効性を評価することが必要である。

(3) システムアーキテクチャを検討する際に考慮すべき点

システムアーキテクチャを検討する際の考慮点の例として、次のような項目が挙げられる（[BSI.3] Annex B)。

a) バックアップサイトの場所とサイト間の距離
b) バックアップサイトの数
c) バックアップサイトのセキュリティレベル
d) バックアップサイトへの業務スタッフの物理的アクセス
e) バックアップサイトへの業務スタッフのリモートアクセス
f) バックアップサイト業務スタッフのスキルレベル
g) サイト間ネットワーク回線の冗長化
h) バックアップサイトへの切り替えの自動化のレベル

(4) その他の関連基準等との整合性

情報システムは、「システム管理基準」、「情報セキュリティ管理基準」、「情報システムの信頼性向上に関するガイドライン」を考慮した開発、運用、変更、保守がなされていることが必要である。

【参考 7： システム管理基準での関連項目】

I. 情報戦略

5. 事業継続計画

IV. 共通業務

7.1 リスク分析

7.3 バックアップ

7.4 代替処理・復旧

5.3 技術的対策

「技術的対策」では、事故・災害等への対策を実現するためのシステム構築技術について例示する。

何らかの理由でシステムが使用できなくなった場合、代替システム（バックアップシステム等）で IT サービスを継続するためには、代替システムを含めたシステム全体のアーキテクチャを事業継続・IT サービス継続の観点で構築する必要がある。

代替システムは、ただ単に既存システムの代替構成を設置するだけでは十分とは言えない。代替システムへのアクセスを可能とするためのネットワーク回線の確保や、既存サイトとバックアップサイトの 2 サイト運用も重要になる。

5.3.1 データレプリケーション方式

代替システムで IT サービスを継続するための最も重要な事項は、どのようにデータを保全するかである。その手段として、従来から、ストレージの機能を使ったデータレプリケーションが良く知られているが、その他、最新の方式について紹介する。

データを同期する方式の選定は、RTO/RPO を検討した上で、システム全体の機器構成･コストパフォーマンスなども考慮した上で行う必要がある。

データレプリケーション方式は、大きく以下の 3 つに分類することができる。以降で説明するレイヤ別方式もこの 3 つの方式に分類される。それぞれ必要されるリソースや注意事項が異なっているのでシステム構成と各方式を充分に検討する必要がある。

a) 完全同期型：メインサイトとバックアップサイトのデータが完全に一致する方式。遠隔地にあるバックアップサイトにも更新を行うためにアプリケーションのレスポンスに影響を与える。
b) 遅延同期型：メインサイトの更新をアプリケーションの処理とは非同期に（遅延して）バックアップサイトに反映する。
c) 一括同期型：データの静止ポイントを確保した上で、一括してデータ複製を行う方式。

5.3.2 システムレイヤ方式

データレプリケーション方式は、ストレージ機能を用いた方式が広く認知されている。しかし、この方式も万能ではなく、様々な要件･システム構成に対応するために図 5.3-1 に示すように各システムレイヤで幾つかの方式が開発されてきた。以降では、これらの方式について説明する。

(1) 運用レイヤ

メインサイトの複製対象のデータをバックアップしたテープを、バックアップサイトへ搬送する方式（図 5.3-1)。具体的には以下のような方式がある。

a) テープによる運用

最も安価な方式である反面、運用に負荷がかかる。受け入れ側バックアップサイトでの運用によって、以下の 2 つに分類することができる。

ⅰ）テープ保管のみ

バックアップサイトではテープの保管のみを行う。災害発生後からデータのリストアを開始することでデータの復旧を行う。

ⅱ）事前リストア運用

バックアップサイトに到着したテープを、バックアップサイト側のシステムに日々の運用の中でリストアを行う。これによりリストア処理時間分の RTO 短縮が見込める。テープを外部へ出すことになるため、搬出用テープの作成・搬出用テープの暗号化などのセキュリティ対策を講じる必要が別途発生する。

b) テープイメージの伝送運用

テープイメージを伝送する方式も、この方式の延長と捉えることができる。テープ媒体を物理的に搬送するのではなく、テープイメージのデータをディスク上に作成しこのデータをバックアップサイトに伝送することで同様の運用が可能となる。

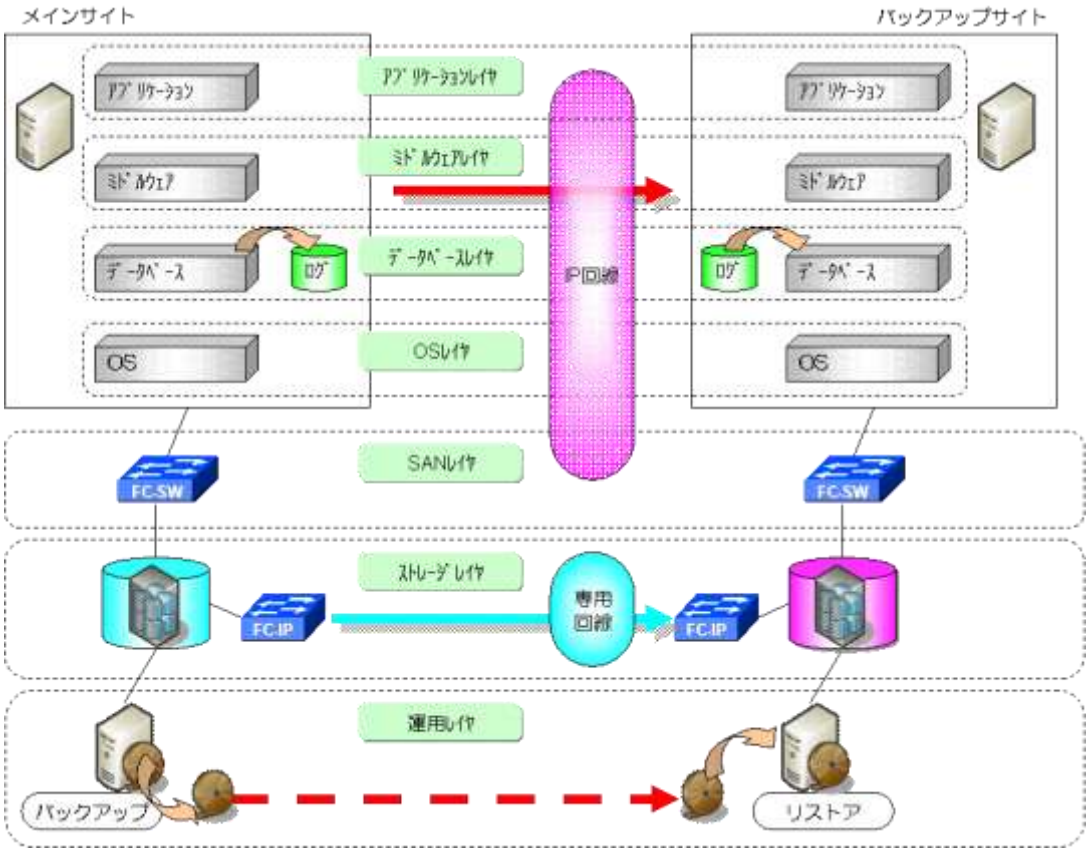

図 5.3-1　システムレイヤ（出典：「NEC 技報　第 59 巻　第 4 号」）

(2) ストレージレイヤ

ストレージ筐体間でデータレプリケーションを行う方式。ストレージが有している機能でディスク上のデータを物理的に複製する。そのため、原則同一機種でのみ複製が可能となる。

(3) SAN レイヤ

SAN アイランドを構成している FC-SW（ Fiber Channel Switch ）及び 相当機能でデータを複製する方式。ミドルウェアレイヤでの方式と同じく、メインサイト SAN 内を通過する I/O データを取得し、バックアップサイト SAN 内で復元することでデータのレプリケーションを実現する。この技術は SAN における仮想化技術の延長とも言える。そのため、異機種ストレージが混在している環境やデータレプリケーション機能を有していないストレージで構成されている環境でも適用することができる。

しかし、システム構成として必ず SAN 構成となっていなければならないため、適用システムに制限が発生する。また、通常の SAN 構成の課題と同じく、SAN 接続性が問題になることがある。そのため事前に接続検証結果を十分に調査しておく必要がある。

(4) OS レイヤ

OS のクラスタリング機能の延長で実現する方式。通常のクラスタリング技術では共有ディスクが必要となるが、クラスタツールで共有ディスク無しでクラスタ構成を実現することができるものがある。この機能を利用し、遠隔地の待機系クラスタノードにデータレプリケーションを実現する。基本となる技術がクラスタリング技術であるため、既にクラスタ環境を導入しているシステムへの適用は比較的容易になる。

(5) データベースレイヤ

メインサイト側データベースの更新ジャーナルデータをバックアップサイト側に転送し、バックアップサイト側のデータベースに反映を行う方式。データベースをジャーナル出力モードで運用する必要があり、そのためにシステムの見直しが発生する可能性がある。

課題として、データベース以外のファイルのデータレプリケーションができない。これが問題となる例として、フラットファイルのパス名のみをデータベースに格納し、フラットファイルは通常のファイルとして管理を行っている構成がある。この構成の場合、データベースはジャーナル運用されているが、フラットファイルはジャーナルで保護されていないため障害時のリカバリ処理で不整合が発生する可能がある。この事象の解決には、業務アプリケーション側で整合性を確保する機能が必要となる。

(6)ミドルウェアレイヤ

ミドルウェアでサイト間データレプリケーションを実現する方式。ミドルウェアがメインサイト側での I/O 処理を取得し、バックアップサイト側で復元するというのが基本的な処理の考え方となる。そのため、ミドルウェアはサーバ OS のファイルシステムに大きく依存することになる。OS バージョンや適用パッチレベルなど、システム環境に大きく依存するため、既存環境への影響も大きくなる。加えて、パッチ適用時の評価確認作業なども増加することになるので、運用面での考慮も必要となる。最近のシステムでは、ミドルウェアのオーバヘッドを意識する必要はない。しかしミドルウェアは稼動するシステム環境と密接に関連を持っているため、他ミドルウェアとの不整合などには充分に注意が必要である。また、レプリケーションの対象となるファイルの特性にも注意が必要で、データの複製単位がファイル単位かブロック単位か等のミドルウェアの機能を意識しておく必要がある。

(7) アプリケーションレイヤ

全ての処理を業務アプリケーションで対応する方式。最も精度を高めることができる反面、最も難易度が高い方式でもある。この方式では、サイト間のデータ整合性を、プログラム間通信やファイル転送などを組み合わせて、アプリケーションで制御することになる。したがって、特に決まった解決策はなく、業務に応じたシステムの構築が必要となる。し

かし、この方式はアプリケーションの基本設計に大きな影響を与えるために、既存システムの拡張という局面での適用は行えず、システム更新などのタイミングでのみ検討が可能といえる。

5.3.3 仮想化技術と構成管理

次に、IT サービス継続を実現するためのシステム構築技術における仮想化技術と構成管理について述べる。

(1) 仮想化技術

代替システム構築の際、メインサイトのシステムに仮想化技術を適用し、分散されたサーバやストレージを統合することで、データやインフラ資産の管理が容易になる。また、本番環境をテンプレート化し、代替システムを迅速に調達・準備することで、復旧期間を短縮できるなどのメリットがある。

(2) 構成管理

メインサイトのシステムと代替システムの構成管理については、従来の最終評価環境と本番環境と同様な管理が必要である。さらに、代替システムの運用では、アプリケーションの構成管理だけでなく、ミドルウェアやハードウェア、さらにネットワークなどの構成についても管理を徹底することが必要であることから、事前のテストが重要となる。

5.3.4 ネットワーク回線

システムの障害対応を実現するためには、サイト間のデータ複製のネットワークを意識しておけばよいが、IT サービス継続を実現するには、以下に示すようなシステムに関連するネットワーク全体を考慮する必要がある（図 5.3-2）。

(1) データ複製用ネットワーク

データ複製を目的としたネットワークである。高品質かつ帯域保証されていることが望まれる。業務にとって不可欠（ミッションクリティカル）なシステムでは、生命線となる重要なネットワークとなる。

(2) 利用者ネットワーク

システム利用者が業務システムにアクセスするためのネットワークである。事故・災害等発生時には、バックアップサイトに適切に切り替えられることが重要となる。同時にセキュリティへの考慮、認証系システムの切り替えも必要となる。

(3) 組織外接続用ネットワーク

社外取引先などとシステム的に連携するためのネットワークである。ネットワーク障害対応を実現するためには、事前に相手先との取り決めが必要となる。

(4) 開発用ネットワーク

事故・災害発生時の障害に対応するために開発環境が必要となる場合は、ネットワークを含む開発環境についてもシステム障害対応に関する考慮が必要となる。

(5) 監視用ネットワーク

運用監視を行うためのネットワークである。2 サイト運用を前提にした環境構築が必要となる。

(6) リモート保守用ネットワーク

サービス提供ベンダーとの調整が必要となる。

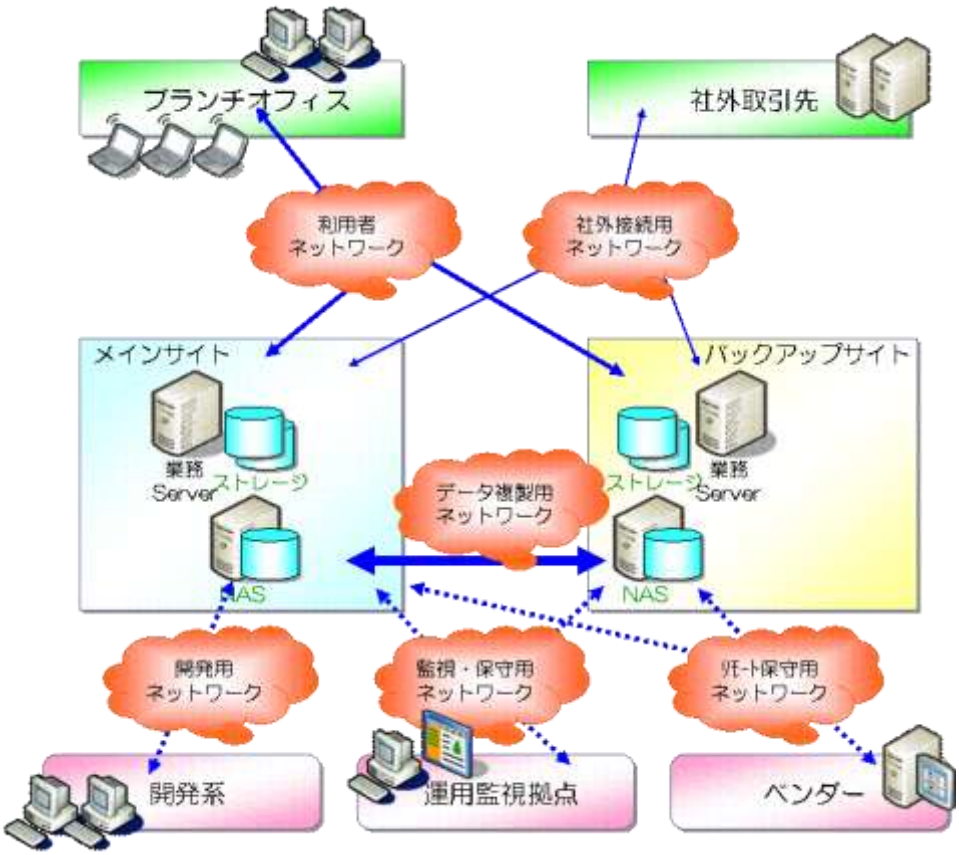

図 5.3-2　システム～ネットワーク関連図（出典：「NEC 技報　第 59 巻　第 4 号」）

5.4 運用的対策

「運用的対策」では、運用上取り得る対策を紹介する。ここでは、管理項目をリソース（経営資源）系とマネジメント系の 2 つに大別して整理した。

運用的対策のうちリソース系の対策としては、

- 従業員
- ワークスペース
- 外部サービス

の 3 分野を取り上げ、また、マネジメント系の対策としては、

- サービスレベル管理
- テスト
- 監査

の 3 分野を取り上げる。

なお、これらの運用的対策は、「5.2 システムアーキテクチャの検討」や「5.3 技術的対策」と相互に関連し、組み合わせて実装されるものであるが、実際に適用される組合せはそれぞれの組織の置かれた状況に基づき、合理的に選択されるべきものである。

また、IT サービス継続マネジメントにおける運用的対策については、次の 3 点を考慮することが望ましい。[BSI.1]

- 継続的な経営管理活動の一環として実施する
- 意思決定機関（注：会議体等を含む）や所管組織等の組織体制を明確にする
- 定期的及び必要に応じて見直す

以下、運用的対策の具体的項目について説明する。

【参照】

[BSI.1]

5.4.1 従業員

緊急事態発生時においては、人命の尊重を第一に考える必要がある。また、IT サービスを継続させるため、人的資源の確保すなわち従業員を効果的に配置することが重要である。以下に、緊急事態発生時における運用的対策のうちの従業員に関する管理項目の例を列挙する。

a) 従業員とその家族の安否や所在の確認方法が定められているか。

⇒ 本人または家族から勤務先へ連絡することを基本とし、必要に応じて勤務先からも連絡するという方法が効果的である。営業時間外の場合、出退状況がわかるよ

うな仕組みを作り、安否確認方法について周知徹底しておくことが必要である。

b) 緊急事態発生時における従業員の連絡網が整備されているか。連絡先は複数明記されているか(自宅電話、携帯電話、携帯メール等)。また、人事異動等は適宜反映されているか。

c) 緊急事態発生時に連絡を必要とする外部組織とそれぞれの連絡方法のリストが作成されているか。特に、重要な外部組織については複数明記されているか。
例（共通）: 警察、消防、監督当局、地方公共団体、業界団体、ライフライン事業者、医療関係先、各種ベンダー、サプライチェーン（取引先)、警備会社、各種設備保守会社、対外接続先　等
例（金融機関の場合）: 日本銀行、全銀センター、CD/ATM 中継センター、近隣金融機関　等

d) 緊急事態発生時における対策本部及び各拠点組織の要員の氏名まで明記した緊急時体制リストが作成されているか。また、組織変更や人事異動等は適宜反映されているか。また、本リストには、必要とする要員のスキルや人数が考慮されているか。

e) システム運用の不測の事態に備えた代替要員の確保が考慮されているか。
⇒ 緊急時体制リスト作成においては、従業員が居住地によっては職場まで出勤できないことも想定されるため、代替要員も含めて検討が必要である。

f) 緊急事態発生時における従業員の招集基準が定められているか。

g) 情報システム運用部門の職務分掌が定められているか。
⇒ 緊急事態発生時における職務分掌の考え方、適用方法について事故シナリオに基づき整理しておく。

h) 代替要員を含む、IT サービス継続のための要員は、適切な教育・訓練を受けているか。

【参照】
[FISC.1]
[FISC.2]

5.4.2 ワークスペース

緊急事態発生時において IT サービスを継続させるためには、その作業を行うワークスペースが必要である。

以下に、緊急事態発生時における運用的対策のうちのワークスペースに関する管理項目の例を列挙する。

a) IT サービス業務を継続するために必要な作業場所や設備は明確になっているか。

⇒ 組織は、復旧時に必要となる活動において要求されるリソースを見積もることが望ましい。必要な作業場所及び設備もその項目として含まれる。必要な設備は、作業場所を見積もる際に要する情報である。

b) 組織は、IT サービス継続戦略の中でワークスペースに対する配慮を行っているか。

⇒ ワークスペースや代替サイトには、組織が所有する場合や、外部の組織との契約による場合などがある。また、システムのバックアップ形態により、コールドサイト、ウォームサイト、ホットサイト、モバイルサイト、ミラーサイトなどがある。それぞれの形態に即して、適切なワークスペースを準備することが望ましい。また、戦略を立てる際には、代替のワークスペースが同一のリスク要因（火災、地震、停電等）を共有しないことや、業務を継続するために必要な人員が、実際に通勤できるようにするための計画を立てるといった点を考慮しなければならない。

※代替サイトには、「自営センター」「共同利用センター」「相互利用センター」「代行処理センター」などがある。

c) IT サービスを継続するために必要なスペースは十分確保されているか。

⇒ ワークスペースや代替サイトを他者と共有する場合は、どれだけのスペースを確保できるかを事前に検討し、必要があれば契約書などに明記しておくことが望ましい。

d) システム及びワークスペースの場所は適切か。

⇒ システムが存在する場所とその他のワークスペースとの距離や代替 IT システムを起動する際に人が介在する必要があるか否かなどについても、戦略策定時に考慮すべき必要がある。

【参照】

[BSI.1]

[BSI.3]
[FISC.3]
[NIST.2]

5.4.3 外部サービス

資材調達、サービス、業務等を外部に依存・委託している場合、緊急事態発生時における外部サービスの継続性は、IT サービスを継続する上で重要な考慮事項である。以下に、緊急事態発生時における運用的対策のうちの外部サービスの事業継続に関する管理について確認することが望ましい管理項目の例を列挙する。

a) 外部サービス提供者の事業継続に関する管理状況を、監査等を行うことにより確認しているか。

⇒外部サービス提供者の委託やサポートを受けている場合、緊急時対応に係る契約条項に、次のような事項が記載されているかを確認する。

例：

優先的にサポートを受けること
外部者との役割分担　等

b) バックアップサイト等を外部に委託している場合、複数の委託元で同時に緊急事態が発生するケースを想定して、外部委託先から受けるサービスが特定されているかを確認しているか。

c) バックアップサイト等を外部に委託している場合、緊急事態時にどのようなサービスが受けられるかなどについて、契約等により明確になっているか、また、その受容したリスクを含む内容を経営者が理解し承認しているか。

d) 事故・災害対策システム立上げや稼動等、バックアップサイト運用に必要な要員の確保の準備はできているか。

e) 外部サービスとの契約における対象範囲や責任分掌等について、明確にしているか。

⇒緊急時対応計画を策定時には、緊急保守サービスに備え、ハードウェア、ソフトウェア、サポートベンダーとの SLA[9]を締結する。SLA では、通知後にベンダーが

[9] SLA（Service Level Agreement）：アウトソーシング先が一定の基準のサービスを提供することを保証する契約で，万

どの程度迅速に対応できるかを特記する。契約には、通常業務用に購入された機器に対する交換用機器の搬送の優先度状態も記載する。SLA には、壊滅的な事故・災害によってベンダーの複数のクライアントが被害を受けた場合の、組織における優先度についても記載する。

f) IT サービス継続のテスト（訓練及び演習等）には、外部サービスも含めているか。
⇒ 演習には、外部サービス提供者の役割を演ずる参加者向けにスクリプト（シナリオ）を作成したり、実際のベンダーの参加者が加わり、代替サイトに実際に移動してシステムの切り替えを行うなどのシミュレーションが大切である。

【参照】
[BSI.1]
[BSI.2]
[BSI.3]
[FISC.1]
[FISC.2]
[NIST.2]

5.4.4 サービスレベル管理

緊急事態発生時において、情報システムのサービスレベルが平常時と同等ではない場合が想定される。例えば、情報システムが全く稼動せず、業務を手作業で行う場合もあれば、バックアップシステムにより、一部の業務が稼動する場合も想定される。IT サービスの継続という観点では、情報システムの稼動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、あらかじめシナリオを策定しておくことが望ましい。

また、外部サービスを利用する場合（「5.4.3 外部サービス」も参照）においては、外部業者との間における契約上に SLA を取り決めておく。SLA については、経営環境や情報システムの状況に応じて定期的に見直しを行う必要がある。

【参照】
[FISC.3]
[FISC.1]

一基準を満たさない場合には保証金をバックするなどの措置が採られる。

5.4.5 テスト・点検

IT サービス継続計画におけるテスト・点検（以下、テスト）の役割は、万一の計画発動における計画の有効性を確認することにある。これは、IT サービス継続計画の発動は極めて稀な非日常の活動であり、日頃から計画実効性を確認することが難しいことから、単なる訓練に止まらず、計画そのものをテストし実効性を確認する作業が必要なためである。

IT サービス継続計画のテストには様々な方法があり、大まかな分類として下表（表 5.4-1）のようなテストの例がある。これらのテストには、様々な分類があり定型化されたものはないため、自組織における IT サービス継続計画の浸透度に適したものを選択すべきである。

表 5.4-1　テストの種類と概要

テストの種類	実施内容	メリット	デメリット
机上チェック	・ 計画の内容をレビューし、不具合を修正する。 ・ 計画に定めた各種内容の有効性を検証する。	早期に実施可能であり、事業への影響が少ない。必要要員も最小である。	対応能力の向上や対応手順の良否の検証は難しい。
ウォークスルー	・ 計画に定めた各種内容の有効性を検証する。	早期に実施可能であり、事業への影響が少ない。必要要員も最小である。机上チェックよりも、より末端の対応手順を検証できる。	計画自身の整合性の検証が中心であり、計画発動時の具体的な課題提示は難しい。
シミュレーション	・ 計画発動時に予想される状況を前提として、計画の実行に必要かつ十分な情報が記載されていることを確認する。	状況を与えることで、より深い計画の検証を行う。あらかじめ与えられた状況内であるが、これに沿って、例えば対応チームごとに対応手順内容を検証できる。	必要要員は多くなる。
ロールプレイング	・ テスト実施の途中で状況を追加付与し、参加者の状況判断や意思決定の可否、連絡体制などを検証する。	計画を実行する判断者の訓練になり、判断資料の手当てなどが確認できる。	想定状況を多数設定するため、事前準備の負荷は大きい。参加者の十分な知識も必要となる。必要要員は多い。
実機訓練	・ 実際の設備などを用いた	代替施設や設備に関して	業務に影響する可能

	テストを実運用及び実作業で行えることを検証する。	実際の手順を適用し、実効性の有無を確認できる。代替システム切り替えなど実際の手順を経験できる。	性があり、周到な準備が必要である。現場レベルで多数の要員確保も必要となる。

IT サービス継続計画のテスト実施で重要なことは、テスト実施そのものが通常システムの稼動を阻害しないようにすることである。このためには、要員手配やテスト後の通常システムへの切り戻しなどについて、十分な時間的余裕を持たせなければならない。そして、テスト計画には通常業務に影響を及ぼす可能性の有無を折り込み、経営層の事前了承を得ることも必要となる。

特に、初めてテストを行う組織においては、テスト計画の策定過程で IT サービス継続計画の矛盾点や不足点、及び安全にテストを実施するための確認事項が多数発見されることも少なくない。このような場合には、テスト実施の延期や縮小など機動的な対応が必要となる。

上述のように、テスト計画の策定自身も、広い意味での IT サービス継続計画のテストと考えられ、各組織においては、テスト計画の策定と実施環境の安全性を早期に確認することが望まれる。

実際にテストを行った組織においては、テストの対象範囲に含まれる以下の事項を検証することが望まれる。

- 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り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

これらの事項について、発見された不具合については、改善の対応部署や責任者を決めて改善計画を策定する。改善方法には、要員やコストなど経営に与える影響が大きいものもあり、経営層の積極的な関与が必要である。

【参照】

[BSI.1]

[NIST.2] IT システムにおける緊急時対応計画ガイド 3.5 テスト、訓練、演習の計画

5.4.6 監査

運用的対策としての、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る。あらかじめ準備した監査計画に従い監査手続を実施し、IT サービス継続に係るリスクに対応した妥当性と、運用の計画事項への準拠性を主な監査目標とする。

IT サービスに関し外部委託を行っている場合には、委託先の状況についての監査が含まれる場合がある。

監査の主な項目は、下記のようなものである。

a) IT サービス継続計画はリスク評価に基づき策定されているか
b) IT サービス継続計画はリスクに対応してそれを統制､低減するものとなっているか
c) IT サービス継続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
d) IT サービス継続計画の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・訓練等が行われているか
e) 外部委託先についても IT サービス継続計画の整備、運用が講じられているか

【参考 8： 金融機関における IT サービス継続】

金融機関は従来より IT サービス継続について体系的に取り組んでいる。以下に示すのは、金融機関における IT サービス継続計画で求められる項目の例である。

・ 災害対策システムは、緊急時対応計画と整合性がとれているか。また、バックアップサイトの保有について検討されているか。
（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 1.）

・ 災害対策システムは、処理業務範囲、機能要件が明確にされているか。
（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 2.）

・ バックアップサイトを検討、構築する際には、次のような事項を検討しているか。
例：
1) 設備
2) システム構成
3) 使用機種
4) 処理能力
5) 外部環境(設置場所、利便性)
6) 運用上の環境(定期テストの可否、スペース、使用時間の制約、データ保管、セキュリティ、互換性、オペレータ要員の確保・訓練、代替サイトで必要となる消耗品、入出力メディア等のサプライ品目の在庫管理/配送等)
7) ソフトウェア管理(代替サイトにおけるソフトウェアのバージョンや修正適用管理、ソフトウェア障害に対する事前予防や遠隔監視/早期対応管理等)
8) 使用形態(専用/共用)
9) 利用コスト(当初費用、維持費用、緊急時使用料)
10) 外部業者利用時の業者のノウハウと実績　等
（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 3.）

・ 次のような事項について、通常運用システムでのシステム変更等が適時に災害対策システムへ反映されているか。
例：
1) 機器構成の変更
2) OS 等基本ソフトウェア、ベンダー提供ソフトウェアのバージョン変更
3) データ、ソフトウェアの更新、変更、削除
4) システム設定値の変更　等

（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 7.）

・ 災害対策システムに係る次のような運用手順書が作成され、緊急時使用可能な状態に保管管理されているか。

例：

1) 災害対策システム立上げ

2) 災害対策システム稼動　等

（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 8.）

・ 通常運用システムとの差異(当初から判明している差異及び通常運用システムの変更の災害対策システムへの反映未了による差異)は管理されていて、災害対策システム稼動時に対応できるようになっているか。

（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 9.）

・ バックアップサイトの施設、機器設備及びネットワークのための安全措置が講じられているか。また、その安全措置は妥当なレベルになっているか。

（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 10.）

・ 災害対策システムには、プログラム修正対応のための開発環境が整備されているか。

（[FISC.2] 11.2.F 災害対策システムーバックアップサイト等の対応 11.）

6. 参照基準

6.1 情報セキュリティ

[JIS.1] 日本規格協会、JIS Q 27001(ISO/IEC 27001) 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

[JIS.2] 日本規格協会、JIS Q 27002(ISO/IEC 17799) 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範[10]

[NIST.1] NIST, SP800-53, Recommended Security Controls for Federal Information systems[11]

[ISO.1] ISO/IEC, TR 18044, Information Security Incident Management

[JIPDEC.1] 日本情報処理開発協会、ISMS ユーザーガイド第 2 版

6.2 事業継続

[NIST.2] NIST, SP800-34, Contingency Planning Guide for Information Technology Systems

[ISO.2] ISO PAS 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management

[CAO.1] 内閣府、事業継続ガイドライン

[METI.1] 経済産業省、事業継続計画策定ガイドライン

[FISC.1] 財団法人金融情報システムセンター、金融機関等におけるコンティンジェンシープラン策定のための手引書第 3 版、平成 18 年 3 月

[BSI.1] BSI, BS 25999-1:2006, Business Continuity Management -- Part 1: Code of Practice

[BSI.2] BSI,BS 25999-2:2007, Business Continuity Management -- Part 2: Specification

6.3 IT サービス等

[FISC.2] 財団法人金融情報システムセンター、金融機関等のシステム監査指針第 3 版、平

---

[10] 11 あるドメインのうち、情報セキュリティインシデントの管理(Information Security Incident Management)と事業継続管理(Business Continuity Management)の 2 箇所で要件を設けている。それぞれについてさらに、前者については、JIS 化されていないが ISO/IEC 18044:Information Security Incident Management という技術文書を発行済みである。

[11] FISMA 法に基づく NIST 文書であり、17 のファミリのうち Contingency Planning と Incident Response という 2 箇所で要件を設けている。

成 19 年 3 月
[FISC.3] 財団法人金融情報システムセンター、金融機関等コンピュータシステムの安全対策基準・解説書、第 7 版、第 7 版追補、平成 18 年 3 月、平成 19 年 3 月（第 7 版が平成 18 年 3 月、第 7 版追補が平成 19 年 3 月）
[BSI.3] BSI, PAS77:2006, IT Service Continuity Management. Code of Practice

【別紙】

IT サービス継続ガイドライン策定ワーキンググループ
委員名簿

（主査）

渡辺　研司	長岡技術科学大学

（敬称略）

（委員）

伊藤　　毅	株式会社富士通総研
織茂　昌之	株式会社日立製作所
佐藤　慶浩	日本ヒューレット・パッカード株式会社
高屋　正裕	日本電気株式会社
田中　　太	財団法人 金融情報システムセンター
西尾　秀一	社団法人 情報サービス産業協会
原田 要之助	大阪大学
藤本　正代	富士ゼロックス株式会社
堀越　繁明	株式会社新生銀行
松原　榮一	社団法人 日本情報システム・ユーザー協会
山本　　匡	株式会社損保ジャパン・リスクマネジメント
和貝　享介	特定非営利活動法人 日本セキュリティ監査協会

（五十音順、敬称略）

（オブザーバー）

経済産業省
独立行政法人 情報処理推進機構
財団法人 日本情報処理開発協会

（順不同）