IT サービス
業務継続ガイドライン

ビジネス継続を支える IT サービス提供のために

2011 年 3 月 18 日発表

レジリエンス協議会 ICT チーム
深谷純子　深谷レジリエンス研究所
伊藤　繁　株式会社野村総合研究所
田代邦幸　株式会社インターリスク総研
黄野吉博　社団法人日本工業技術振興協会

はじめに

インターネットをはじめとするコンピュータシステムの発達により、今やビジネスに IT サービス（Information Communication Technology Service：ネットワークに接続したコンピュータシステムによるサービス）は不可欠になっており、IT の途絶による業務停止や IT サービスの不正使用や情報漏洩は、企業の事業運営に多大なインパクトを与える。

IT サービスの業務継続性は 1980 年代から専門家の中では大きなテーマとして取り上げられ検討も進められていたが、2001 年 9 月 11 日に発生した米国同時多発テロをきっかけに IT の専門家以外のビジネスマン、行政関係者にも IT サービス中断の脅威を広く認識させることになった。

9.11 以降、我が国でも日本銀行と経済産業省を中心に IT の業務継続性が調査され、2003 年から 2005 年にかけて、次のようなガイドラインや論文が発表され、IT の業務継続計画書（IT-BCP）の普及に一役を担うことになった。

「金融機関における業務．継続体制の整備について」 日本銀行、2003 年 7 月
「金融市場における業務継続体制」 日本銀行、2003 年 9 月
「当取引所の BCP について」 東京証券取引所、2004 年 6 月
「事業継続計画策定ガイドライン」 経済産業省、2005 年 3 月

その後、IT を包括する企業全体の BCP の普及が内閣府や中小企業庁を中心にはじまったが、IT-BCP と企業全体の BCP とが混在するようになり、一部ではその両者の違いに対する当惑も見受けられるようになった。

そこで本書では、IT-BCP に特化して解説を試みることにした。企業全体を対象とした BCP では自然災害や新型感染症の想定がよく知られているが、IT サービスではオペレーションミス、プログラムエラー、パフォーマンス低下などの方が、発生頻度は高く、業務停止を引き起こす脅威となっている。

本書で、IT サービス継続として取り組むべき脅威を復習し、IT-BCP を作成する際の観点を明確にしていただけると幸いである。

2011 年 3 月 10 日
深谷純子

目次

第 1 章　IT の業務継続に関する規格

ICT の業務継続に関する規格としては次の二つがある。

- 『ISO/IEC 27031：Guidelines for Information and Communication Technology readiness for Business Continuity』、2011 年 3 月
- 『BS25777：Information and communications technology continuity management --- Code of practice』、2008 年 12 月

前者は国際規格（ISO）であり、後者は英国規格であるが両規格の類似性は高い。本書の解説は、BS25777 を基本にしているが、ISO/IEC 27031 で改定、修正された部分を一部含んでいる。

読者のためには『ISO/IEC 27031 の解説書』と明記したいところであるが、ISO/IEC 27031 の公表から日数が少ないため、ISO/IEC 27031 に対しては不完全な解説に留まっている。本年（2011 年）の 10 月頃には完全な解説書に書き換える予定である。なお本書では、上記両規格を日本語で次のように表記する。

- 『ISO/IEC 27031：ICT の業務継続』
- 『BS25777：ICT の継続性マネジメントに関する実践規範』

第 2 章　IT-BCP と事業全体の BCP

次のとおり英国規格にも国際規格にも、前述の IT の業務継続とは別に組織全体（以下「ビジネス」）の事業継続に関する規格がある。

- 『BS25999-1：事業継続管理のための実践規範』、2006 年 11 月
- 『BS25999-2：事業継続管理のための仕様』、2007 年 11 月
- 『ISO22301：事業継続マネジメントシステム（BCMS）』、現在審議中

なお、BC、BCP、BCM、BCMS は次のとおりそれぞれ意味が少し異なっている。

- BC：「業務継続」または「事業継続」
- BCM：「業務継続マネジメント」または「事業継続マネジメント」で BC に対する包括的な取り組み
- BCMS：「業務継続マネジメントシステム」または「事業継続マネジメントシステム」で BC に対する包括的な取り組みを組織的・継続的に実行する仕組み
- BCP：「業務継続計画書」または「事業継続計画書」で BCM の成果物のひとつ

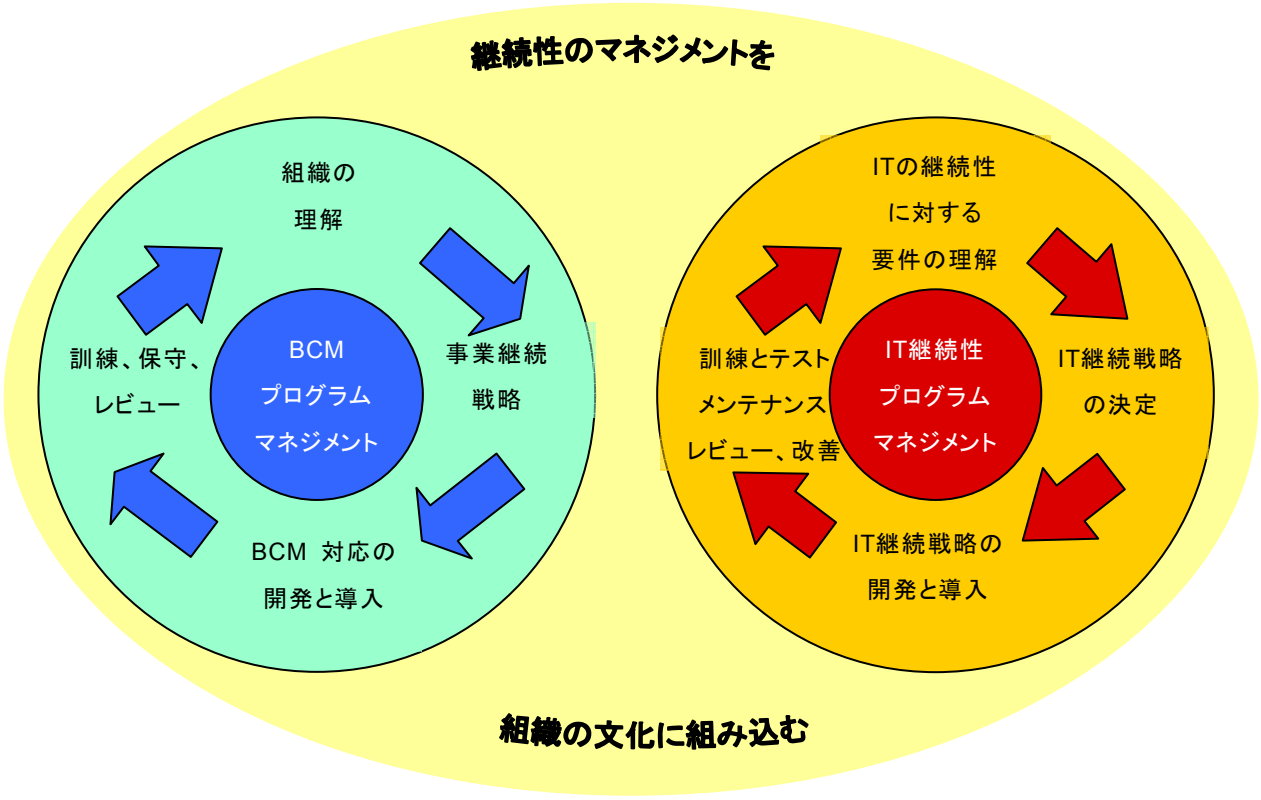
ビジネスの BCM においては、業務影響分析（BIA）などを経て、その組織の事業継続性に対する要件を見出していくが、多くの業務が IT に依存しているため、ビジネスの要件には必ず IT サービスの継続が必要になる。

2.1 ビジネス継続と IT 継続のマネジメントサイクル

図表 1 はビジネス継続と IT 継続の関係を表したものである。図の左側が BS25999 で推奨されているビジネスの事業継続マネジメントへの取り組みのサイクルであり、これに対応して図の右側が IT の業務継続マネジメントへの取り組みのサイクルである。これはビジネス側のサイクルを回すと、必然的に IT 側のサイクルも回ることを示している。

逆に IT 側のサイクルを回すとビジネス側のサイクルも回る。例えば、社内の入力データフォームを統一化すると、ビジネスの分類や進め方が変わる。

図表 1 ビジネス継続と IT 継続のマネジメントサイクル

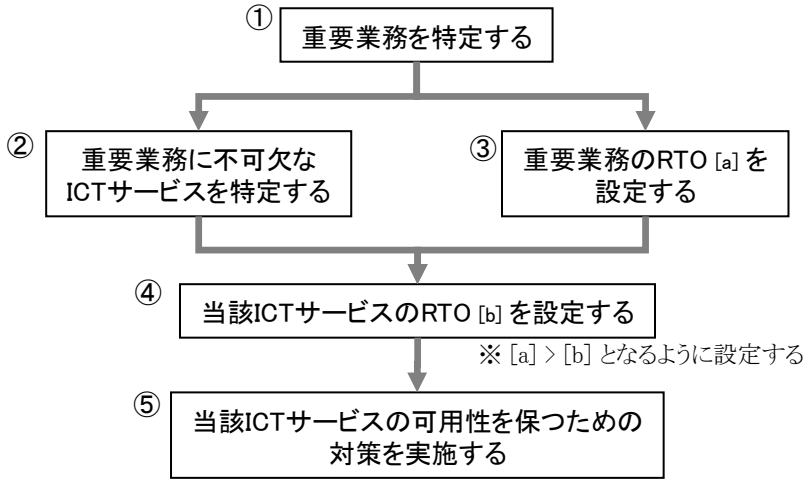


（出展：BS25777）

2.2 IT 継続マネジメントにおける検討プロセス

図表 2 は、IT 側のサイクルにおける検討プロセスをもう少し具体的に表したものである。この図表で①から③までは、ビジネスにおける BIA で取り扱われる部分に相当する。更に検討を④、⑤に進め、IT 継続に対する要件を明らかにしていく。

図表 2 IT 継続マネジメントにおける検討プロセス



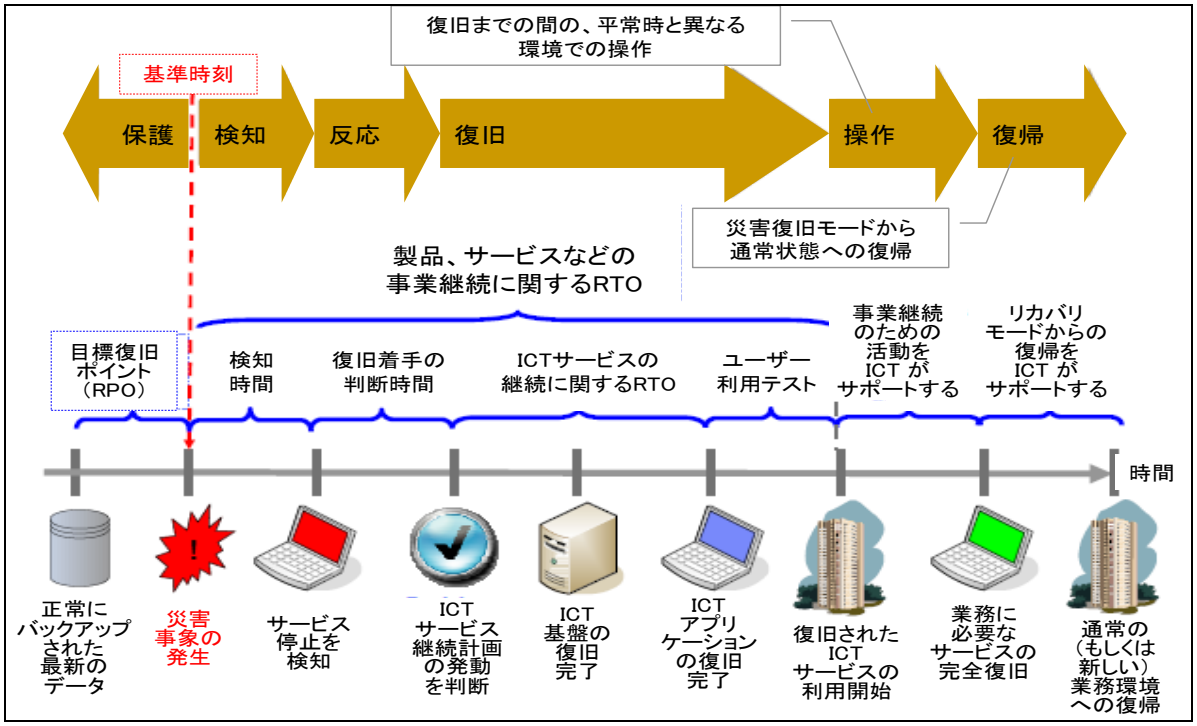
図表 2 の⑤では、IT サービスを早期再開・復旧させるために、計画・マニュアルの作成や、機器に対する対策（冗長化やデータの保全等）といった対策が必要になる。BS25777 および ISO/IEC 27031 では、実際の対策に関して留意点が列挙されているが、具体的にどのようにすべきかといった詳細なガイドラインは示されていない。もし詳細なガイドラインなどが必要であれば、例えば次のような文書を必要に応じて併用することになる。

- ISO/IEC18043: 侵入検知システムの選定と運用
- ISO/IEC24762: 災害時復旧サービス
- ISO/IEC27035: 障害対応手順

2.3 RTO の設定

ここで IT サービスの RTO（目標復旧時間）を設定するにあたり、図表 3 の構造を理解する必要がある。早期再開・復旧すべき業務が特定され、それに対する RTO が設定されたら、その RTO より短い時間で、必要な IT システムが稼働する必要があり、かつ障害が発生したことを検知する時間や復旧作業に着手するまでの時間（および判断のために必要な情報を収集する時間）、再開・復旧後のテストを行う時間も含めて考えなければならない。

図表 3 RTO（目標復旧時間）の設定



（出展：BS25777）

なお、BS25777 および ISO/IEC 27031 が目指すものは、ビジネスにおける IT レジリエンスの最適化であり、闇雲に IT のレジリエンスを上げることが目的ではない。IT レジリエンスの維持向上のためにかかるコストが過剰に膨らむことは避けるべきである。

第 3 章　他の規格との関係

3.1　ISO/IEC 27001/27002

情報セキュリティに関する国際規格である。この規格の中で、情報セキュリティは情報の「機密性」、「完全性」および「可用性」の維持であると定義されている。この規格には、「可用性」の一部として「事業継続管理」という項目があるが、対象はシステム障害やセキュリティインシデントに起因する事業中断事象を対象としており、必ずしも大規模災害等を想定したものではない。

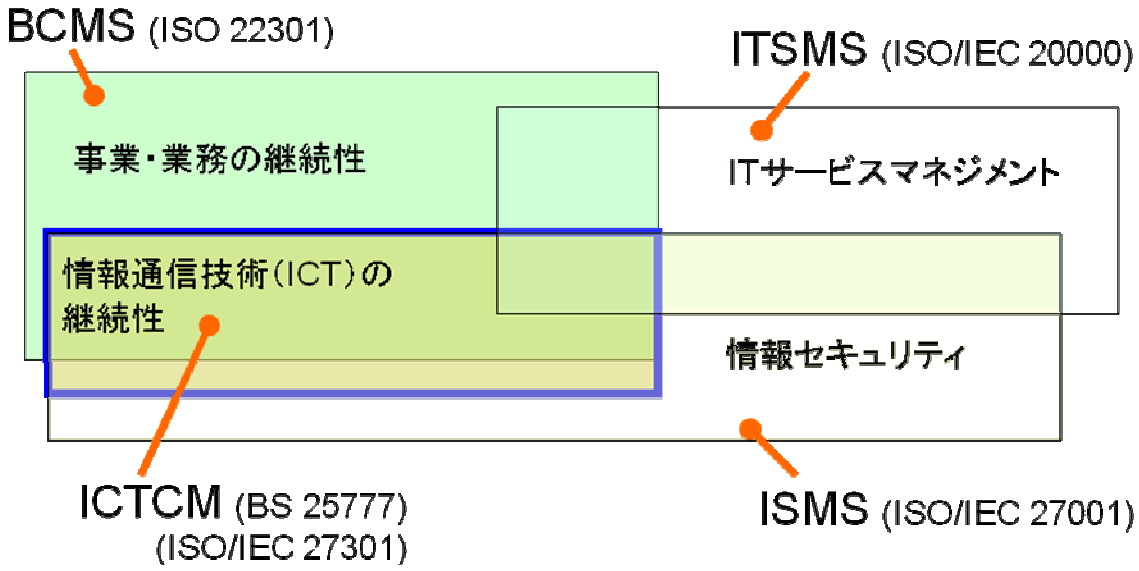
しかしながら、この規格で事業継続管理のために推奨されている手法は、ビジネスの事業継続ガイドライン（第 2 章参照）で推奨されているものと類似している。

3.2　ISO/IEC 20000

IT サービスマネジメントに関する国際規格である。この規格では、組織内外のユーザに対して提供される IT サービスの質を継続的に維持するために、IT サービスの提供者が実施すべき管理策が整理されている。この中で、「サービス継続及び可用性の管理」というプロセスが、IT 継続管理（IT-BCM）と最も関係が深い。

また、「サービスレベル管理」というプロセスには、ユーザとの間でサービスレベルの合意形成が含まれているが、これはビジネス要件と IT サービスのレジリエンスを整合させることに相当する。従って IT サービスマネジメントの枠組みの中では、「サービスレベル管理」と「サービス継続及び可用性の管理」との二つの管理プロセスの組み合わせによって、IT-BCM の概念が具現化されていると見ることができる。

図表 4　関係規格の位置付け



第 4 章　IT の BCP 策定について

本章では、組織が目指すビジネスの事業継続目標を実現するため、IT 部門としてどのような取り組みが必要か、その要件を整理する上でのポイントを解説する。

4.1　ビジネス・法的・契約など IT-BCP の要件定義

IT-BCP の戦略および計画を策定する上の前提条件を明確に整理する。具体的には、組織がどの事業を優先的に継続・再開しようとするのかを明確（対象業務とその目標復旧時間や復旧レベル）に整理する。また、事業の遂行上遵守または考慮する必要がある法的要件や、各種契約条件を洗い出し、組織としてビジネスの継続方針と IT-BCP の方針の整合性を確実にする。

4.2　IT の評価基準の設定

組織のビジネス継続目標を達成するため、ICT に関する業務継続能力のレベルを評価する基準を設定する。ここで、IT-BCP 策定の検討を開始するにあたり、IT 部門としてのミッションと、IT の業務継続に関する実力を評価するための基準を作成することが必要になる。ビジネス側で規定される優先継続業務とその時間的要件が、IT-BCP の検討を進める上での、前提条件となる。ビジネスの BCP 方針と齟齬が無いよう、最低限、以下の 4 項目について明確にする必要がある。

a. ビジネス側で決定された、優先継続業務
b. 優先業務の目標復旧時間（RTO）
c. 優先継続事業の目標復旧ポイント（RPO）
d. IT-BCP を検討する上で、契約上また法的に遵守または考慮すべき事項

なお、バックアップされたデータを利用して業務を再開した場合、RPO 以降に書き込まれたデータが欠損した状態で ICT サービスを再開することになるため、欠損（最終静止点以降に発生）したデータの復元方法について、ビジネス側との連携が必要となる。また、ビジネス側の BCP 発動時や災害時・緊急時にのみ使用される ICT サービス（安否確認、緊急時通信・連絡機能、緊急時用広報機能など）に対する要件を検討する場合も、ビジネス側の要件と整合性を確認する必要がある。

また、IT の評価基準の設定については、IT の構成により項目が多岐にわたるが、少なくとも以下の項目を含める必要がある。なお、評価基準はビジネス側が要請するレベルを数値化するか、または求められる整備状況に対して現状を○／△／×などの記号で評価できるようにする。

- ビジネスと IT サービスの対応の分析とその文書化
- 継続対象業務に必要な機器・アプリケーション・データの分析とその文書化
- 最新の IT ネットワーク構成図、各種管理表の整備状況とその更新状況

- IT 各システム（最低でも優先継続対象システム）で使用するデータの、分散配置状況と、バックアップ周期（RTO）
- 想定するリスクによるシステム被害が発生した時の、被害想定および再開見込み時間
- バックアップシステムの立ち上げ時間（最新の訓練または実例での計測）
- バックアップシステムの立ち上げ訓練実施状況（過去の訓練テーマとその結果分析による課題抽出状況とその取り組み状況）
- 優先継続業務に関わる、保守委託先やアウトソース先との SLA の設定または契約書への、業務継続要件の記載などの実施状況
- ビジネス側が求める要件と現状の IT-BCP の実力との乖離状況に関する分析とその結果（問題点、潜在リスクなどを含め）とその文書化、および経営層への報告と報告結果（指示または承認）の記録

第 5 章　IT-BCP の検討に必要なリソース

組織は、ビジネス側の目的を達成するための一要素として、IT-BCM プログラムを認識し、策定・実施・運用・維持に必要な、リソースを確保する必要がある。また、IT-BCP が取り扱う範囲、ビジネス側の BCP との役割分担、IT-BCP の遂行に必要な外部組織（アウトソース先、修理業者、インフラなどサービス提供者など）を文書化する必要がある。また、経営層は、IT-BCM を推進するための体制を確立するため、以下を行う。

- IT-BCP の計画策定および運営責任を持つのに相応しい、経験と権限を持つ人材の指名
- IT-BCM を構築・維持運営するための、有能な人材の配置

IT-BCM を推進するための体制（IT-BCM 推進委員会／事務局／担当など）は、経営層が指名する。この指名は、組織としての事業継続方針を実現するための取り組みを、各部門が推進する裏に経営層の強い意思があることを認識させ、各部門が同じベクトルで、事業継続の取り組みを推進するための、重要なポイントとなる。

5.1　IT-BCP の検討に関わる人的要件

IT-BCM を推進する人材は、それに必要な経験と知識を持っていることを確認の上、選定する必要がある。また、必要な経験と知識が社内で不足している場合は、候補者に対する研修や訓練を通じた人材育成、また、外部からの支援といった方策を取ることを検討する。

5.2　IT-BCP に対する要件定義

組織は、ビジネス側の BCP の一要素として、優先的に継続すべき業務（BIA 分析に基づく）に応じて業務を分類する必要があり、それらの業務の再開時におけるレベルを規定する必要がある。経営層により承認された、ビジネス側の事業継続要件に基づき、重要継続業務毎に RTO、RPO および必須業務継続目標（MBCO; Minimum Business Continuity Objective）について文書化する。なお、文書化の際はヘルプ・デスク機能および次の項目を含める。

- ICT サービスの名称は統一し、ユーザ部門と IT 部門との整合性
- ICT サービスの簡単な機能説明
- ICT サービスとビジネス側が生産する製品やサービスとの対応表

ここで、IT-BCP の要件定義として、以下のポイントが必要になる。

(1) 経営層により承認された、全社 BCP に基づく業務要件の文書化

優先すべき業務とその達成要件である RTO、RPO、再開時の稼動レベルなどを、IT 部門の視点

で明確に整理すること。

(2) IT サービスに関するインベントリの作成

組織が、どのような IT サービス機能を持っているかについて、分析し文書化すること。特に IT サービスと各業務(製品やサービス: 在庫管理、顧客管理など)との関係が対比できる分析が必要となる。これは、H/W 障害が、どの業務に影響するかを速やかに認識する上でも有効となる。

5.3 重要 IT サービスの認識

経営層により承認された重要な IT サービスに関する、エンドツーエンドサービスでの IT 構成要素;設定・接続状況について、文書化する必要がある。また、通常状態で使用される IT サービス提供環境と、IT 業務の継続(DR 的)環境について、その構成を文書化する必要がある。

重要な IT サービスに関しては、サービス中断または低下の予防の観点から、リスク評価の中で、現状の継続能力について、例えば、単一障害点(Single Point of Failure)を見直しすることも必要になる。また、IT サービスの継続能力は、ビジネス側のリスク分析作業の中でも取り扱う必要がある。

また、一連の分析作業を、IT サービスのレジリエンス向上や、サービスの中断の影響の軽減に関する検討、さらに IT サービス中断に関する早期発見・対応といった改善の機会と考え、これらの調査を踏まえ、組織は IT サービスのレジリエンスの向上に関する事業投資判断を行うことが可能となる。これらサービス・リスク評価は、IT サービスの復元能力強化のための事業審査項目として提示される。

更に、重要な IT サービスを認識するため、IT の構成要素レベルまで、分析することが必要となる。IT サービスに必要な要素である、H/W、S/W、ネットワーク、データ、運用などのレベルまで分析し、文書化する必要がある。この分析の中で、単一障害点の認識や、各機能間の相関関係などについても、併せて実施する。

プライマリ側/バックアップ毎のシステム環境について、記述するとともに、その相互関係(データの転送周期やデータの静止点など)についても、明確にしておく必要がある。

5.4 IT の現状能力と事業継続要求レベルとのギャップの認識

重要 IT サービスに関する現状(例えば、予防対策、稼動監視、異常検知、対応・回復能力など)について、事業継続の要求レベルとの比較およびそのギャップを、文書化する必要がある。

経営層に対しては、ビジネス側が求める能力と IT-BCP の現状とのギャップを報告する必要がある。その報告では、想定されるリスクや追加すべきレジリエンスおよびリカバリに必要な資源について、記述する必要がある。なお、リカバリに必要な資源としては次がある。

- 要員(人数・必要となる技術・知識を含む)
- IT 設置関連施設(コンピュータ室など)
- システム・装置、ネットワークなど

- アプリケーション・ソフトやデータベース
- 資金または予算配分
- 協力会社および部品・消耗品供給会社
- その他

経営層は、IT サービスの定義、文書化された重要 IT サービスおよび全社事業継続が求める要件と IT 能力の現状との、リスク面でのギャップを認識した上で、サインオフする必要がある。この中には、IT-BCP で認識されている、リスク情報についての記述を含む。なお、ここで想定リスクに対する IT サービスの影響とビジネス側が求めるレベルとの乖離(プラス・マイナス両方向)を確認する必要がある。確認すべき項目は、一般的に人・施設・システムデータといった要素になる。ギャップ分析する場合、まず、想定するリスクが出現した場合、IT に関わる、リソース(以下に一般的な項目を示す)に、どの程度の被害が発生するかについて、分析し、その上で、既存のシステム環境が、どの程度のレジリエンスがあり、ビジネス側の期待レベルとの乖離が、どの程度かを分析することになる。

① 人的要素の分析

- 社内外に関わらず、再開時に必要となる、システム運用・保守・開発要員の人数と、リスク出現時の参集想定数
- 各要員に求められる、技術レベル・知識・資格要件の現状と、リスク出現時に想定される課題

② 施設要素の分析

- 重要なITサービスを提供するためのシステムを設置する場所や、システムを運用・監視するための場所(データセンタやサーバルーム・システム運用監視室・コマンドルームなど)
- 該当場所の、電気・通信などの冗長性・耐震性、UPS や発電機の容量や連続運転時間、電源供給能力(ラック当り供給能力)と稼働率、空調能力、その他リスク出現時の影響

③ システム要素の分析

- 重要な IT サービスを提供するための、H/W・S/W とその代替性(想定障害レベルと復旧見込み時間、H/W 新規購入時の既存アプリの互換性確認など)
- 通常使用しているシステムが停止した場合の、代替設備への切替所要時間

④ データ要素

- データのバックアップ対策の実施状況と、リスク出現時の影響
- データのリカバリ時間と、RPO 以降発生したデータのリカバリ方法
- システムのプライマリ側への切り戻し時の、データのリカバリ方法など

⑤ 業務委託関連

- 重要 IT サービスに関わる、重要委託先の分析
- 委託条件(SLA や BCP での RTO の整合性確保)と全社 BCP 要件との乖離状況
- 合意されている、SLA または RTO の、想定リスク出現時の影響
- 合意されている、SLA または RTO を維持するための仕組の裏付確認

第 6 章　IT 業務継続戦略レベルの決定

IT 業務継続戦略、IT に求められるレジリエンスを実現するための取り組みを規定する。この取り組みにより、障害予防・検知・対応・復旧・復元といった機能を、ビジネス側が求めるレベルで実現する。

戦略を検討する際、ビジネス側は、初期構築分だけでなく、継続的なリソース要件に関する費用を考慮する必要がある。また、戦略策定支援のための専門サービスや、技能を持つ外部の専門家の使用についても、必要に応じて考慮する。

IT 業務継続戦略は、マーケット毎に異なるビジネス戦略にも柔軟に対応出来るよう考慮すべきであると共に、以下のような社内的な制約や要因についても考慮する。

- 予算
- リソース状況
- 想定されるコストとその効果
- 技術的制約
- 組織のリスクに対する考え方
- 組織の既存 IT 業務継続戦略
- 法的義務

組織は、IT サービスの障害に備え、充分な検討を行う必要がある。オプションとして、障害防止およびレジリエンスの向上や計画外の中断からの復旧・復元、組織に対する IT サービスの提供、外部ベンダにより提供されるサービスに関する社内調整、といった点も考慮する必要がある。また、戦略を実現するためのオプションは、IT サービスの継続と復旧を確実にするために必要となる、項目全般を対象範囲とする。

6.1　必要となる技術と知識

組織は、中核として維持すべきIT技術と知識について、戦略を考慮する必要がある。これには、従業員・契約社員だけでなく、IT-BCP 運営に必須の委託先など、特別な知識・技術を持つ専門家を含める。それらスキルの提供または保護のための戦略は、以下のものを含む。

- 重要な IT サービスがどのような技術により提供されているかの文書化
- IT 担当者や契約社員に対するマルチ・スキル化訓練
- リスクの集中を削減するためのコアスキルの分離（コアスキルを持つ担当要員の物理的な分離や、コアスキルを持つ要員の育成など）
- 知識レベルの維持と管理

6.2 施設

組織は、日常的に使用する IT 用施設の機能停止による影響を縮小するため、戦略を検討する必要があり、検討すべき対象事例は、以下のとおりである。

- 他の業務を停止して確保するものを含む、組織内の代替施設（場所）
- 他組織から供給される代替施設
- 専門の業者から提供される代替施設
- 自宅または遠隔拠点からの業務
- その他予め調整・合意してある、適切な作業場所
- 既存の代替労働力の使用
- 障害現場に搬入可能な代替設備および物理的資産の一部で直接置換可能な物

IT 関連施設に関する戦略は、極めて多様かつ広範囲な選択肢が利用可能といえる。異なるタイプの事故や脅威のため、複数の戦略を選択し組み合わせることが必要となる。この戦略は企業規模、事業範囲、拠点、技術、予算などにより、限定的な運用になることもある。なお、代替拠点の使用に関しては、以下の点について考慮する必要がある。

- 拠点のセキュリティ
- スタッフの通勤手段
- 既存施設との近接性
- 利便性

6.3 技術的要件

重要業務に必要な IT サービスは、その重要業務を再開する前に、利用可能状態になっている必要があり、この対応策としては規定の時間枠（例： BIA で定められた RTO）以内にアプリケーションが確実に利用可能となるよう、考慮する必要がある。このため必要となる、ハード環境やアプリケーション・ソフトの RTO は、ビジネス側が求める時間軸内に設定される。

IT サービスを支える技術は、継続性を確実に維持するため、しばしば複雑な設定・調整を必要とする。IT 業務継続戦略の検討時、以下のような項目について配慮する必要がある。

- 全社 BCM プログラムで特定された重要業務が必要とする、IT サービスの RTO と RPO
- 技術拠点の場所およびそれらの距離
- 技術拠点の数
- システムへのリモートアクセス
- 空調要件
- 電源要件
- 有人サイトに対し無人（ダーク）サイトの使用

- 通信の接続性および異経路
- 「障害時立ち上げ(failback)」の属性 (代替 IT 設備の立ち上げの手動・自動)
- 自動化レベル要件
- 技術の老朽化
- アウトソースサービス提供者との接続およびその他外部連絡線

6.4 データ

重要業務は、最新またはほぼ最新のデータの確保に依存する。データの継続性に関する対策を検討する上では、ビジネス側で規定された重要業務が求める復旧ポイント目標(RPO)を満たすよう設計することが重要となる。選択された IT-BCP のオプションは、継続的な機密性・信頼性・可用性の確保(ISO/IEC27001 および ISO/IEC27002 を参照)や、重要業務が必要とする最新の重要データを確実に提供する必要がある。

データ蓄積と IT 業務継続戦略は、全社の事業継続要件と整合している必要があり、また、以下の項目について考慮する必要がある。

- RPO 要件
- データの安全な保管(例: ディスク・テープや光学メディアの保存)、適切なデータ・バックアップおよび復元機能による、確実なデータの保証
- 拠点内、拠点外または第三者などによる情報の保管場所、搬送または伝送・距離・場所、ネットワーク接続、バックアップ・メディアからの復旧にかかる想定時間
- データ量、データの保管方法、技術的な復元手順の複雑さ、ユーザ側や全社的な復旧要件などに影響される、復元時間

組織内でのエンドツーエンドデータ利用の理解は、極めて重要である。これには外部との情報授受を含め、考慮することになる。組織内でのデータの特性・最新性・価値は、劇的に多様化していることに、留意する必要がある。

データのリカバリにおいては、システム毎に RPO が異なる恐れがある点に、留意が必要となる。バッチ処理を行うホスト系システムでは、一般的に、RPO が 24 時間となる一方、サーバ系 DB では、リアルタイムに近い RPO を持つケースがある。このようなホスト・サーバ混在型システムを立ち上げると、サーバ側は直前のデータで再開し、ホストは前日の状態で再開することになり、DB 間で矛盾が発生する可能性がある。データの復旧に関しては、システム間のデータの整合性という点についても、充分考慮した設計が必要となる。

また、復元したデータを使用して業務再開する場合、データが想定した状態にリカバリされているかを確実に検証する手順が必要となる。不十分な状態でリカバリされたデータに新たなデータが積算されると、その復旧は極めて困難となり。システム立ち上げ完了後、各業務部門に正常性の確認を依頼し、業務側での確認完了を受け(業務側の事業継続手順にも、データの正常性を検証するための手順が必要となる)、通常業務を再開するといった手順が必要となる。

6.5 プロセス

IT 業務継続戦略を選定する際、組織は障害の予防・検知・回復や災害復旧といった、戦略の実効性を確実にするために必要なプロセスの要素（例えば、重要な技能、重要データ、必須技術、重要装置および施設）を考慮する必要がある。

6.6 サプライヤ

組織は、IT サービスの運営に必要となる外部依存性を分析し、文書化する必要がある。また、組織は、第三者により提供される重要な装置またサービスについて、予め定めた時間軸内に確実に提供されるよう、適切な手順を取る必要がある。

このような依存性は、ハードウェア、ソフトウェア、回線、アプリケーション・ソフト、外部のホスティング・サービス、ユーティリティ、さらに空調や環境モニタリング、消火といった環境維持といった、以下の項目が想定される。

- 他の場所での、追加設備やソフトウェアコピーの保管
- 装置の配送および交換作業の即時対応に関するサプライヤとの調整
- 装置不具合が発生した場合の、迅速修理や故障部品の交換
- 電力や通信回線の二重（冗長）供給
- 緊急発電装置および
- 代替/予備供給者・供給方法の事前調査

組織は、パートナーやサービス提供者との契約に、IT と BCM 要求を含めなくてはならない。契約明細には、それぞれの組織の義務、合意されたサービスレベル、主たる障害に対する対応、費用分担、訓練の頻度および是正措置などについて、反映されている必要がある。

ビジネス側で継続対象となった業務に必要な IT サービスに関しては、その IT サービスの継続に必須となるアウトソース先や協力会社との間で、上記のような合意を形成する動きが増加してくるものと想定される。具体的には、入札時に要件が提示され、予めサービスレベルを維持するための、仕組みの説明なども含め、説明責任が求められることも想定される。さらに、契約においても、事業継続性に関する規定が明記され、継続性を確実に履行するための取り組みが求められる動きが増加している。

6.7 サインオフ

IT 業務継続戦略に取入れられた方針は、リスクの影響と戦略実現に必要なコストを基本にした、決裁のための推奨案を付して、トップマネジメントに報告されなくてはならない。もし、IT 業務継続戦略で取り入れられた対策が、事業継続要件を満たさない場合は、現行の継続能力と合わせ、トップマネジメントに報告されなくてはならない。

トップマネジメントは、オプションとして報告された IT 業務継続戦略を選別し、選択した項目が、適切に実行され全体の事業継続要件を満たすものであることを文書化した上で、承認・署名する必要がある。

IT 業務継続戦略オプションは次のとおりである。

- 起こりうるリスクや中断による影響を考慮されなくてはならない
- 組織の事業継続戦略と統合されなくてはならない
- リスクの範囲で、組織全体の目標に合い妥当でなくてはならない

IT-BCP の検討の過程で、バックアップシステムの構築・耐震性強化・データ・バックアップ機能の改善、ネットワークの冗長化など、多くの課題が出現する。この時、どの対策を採用し、どこまで取り組むかは、リスクの発生確率と、その対策を講じなかった場合の影響の大きさを経営層に報告し、判断を受けることになる。リスクを軽減または回避するための対策の要否判断は、ビジネス側の問題であり、対策を講じないことにより潜在化するリスクを含め、経営層は正しく認識した上で、サインオフする必要がある。
この時、経営層は、組織の事業継続要件に対し、ICT 側の対策がどこまで実現され、何が潜在リスクとして残ることになるかを、書面で確認することになる。また、ICT 側は、経営に対し、潜在リスクを除く範囲で、重要業務に必要な ICT サービス提供者として、全社的なビジネスの事業継続を実現するための一翼を担う責務を負うことになる。

6.8 IT 業務継続能力の強化

組織は、長期的な IT 業務継続戦略の中に、IT-BCP で求められる要件を満たすために必要な、IT の業務継続能力の具体的な強化項目などを上げておく必要がある。このような強化は、予防対策や改善策と同時に、組織的に行われる BIA やリスク分析といった、他のプロセスや手法の結果からの要請として達成される。

組織が求める事業継続性を実現する上で、IT-BCP 側で改善すべき事象を、長期的な視点で、徐々に改善強化するべきであるというのが、ポイントである。初期の IT-BCP 整備の中では、予算や要員事情から実施することが出来ず、潜在リスクとした項目に対し、長期的な視野で対応方針を策定し、対応可能な範囲から、徐々に実施することで、IT-BCP の強化を図る。

6.9 IT 対策パフォーマンス評価基準

どんな ICT 環境にも、ハードウェア障害、セキュリティ侵入など多くの潜在的な脅威がある。従って、組織はそれらの脅威を監視し、それらの脅威に対して適切な対応能力があることを、確認するべきである。

また、組織は ICT 対策の効果を測定するための、パフォーマンス評価基準を定義すべきである。このようなクライテリアは、効果的・効率的両観点から、中断時の対応に求められる品質の決定に使われる。IT-BCP のためのパフォーマンス評価基準は、障害対応や継続要件に関する全社的 BCM と同様に、

IT-BCP で求められる要件に基づいていなくてはならない。なお、この評価基準を設定するためには、少なくとも以下のポイントをカバーしていることが必須となる。

- 優先継続業務の継続に必要な ICT サービスの分析
- 継続すべき ICT サービスの、想定リスクに対する影響度分析
- 組織が求める優先継続業務の RTO と、対応する ICT サービスが持つ RTO の対比
- 障害直前のデータ回復に関わる、RPO とのギャップの整備状況（業務部門でのデータ再投入手順などの整備）
- 重要な ICT サービスの継続に必須な、外部委託先、協力会社との、災害時における業務継続に関する SLA などの設定と契約状況

また、多様なリスクに対する対応状況の検討には次を含める。

- バックアップデータの蓄積・保管状況と、同時被災が想定されないことに関する検証
- 重要 ICT サービスに関わる要員の必要技能・技術・資格の洗出しと、現状分析
- IT-BCP に関する演習の実施状況
- IT-BCP の潜在リスクと潜在リスクに対する対応方針およびその進捗状況

第 7 章　実装と運用

IT 業務継続戦略の実装は、経営層による承認の後にのみ、実施すべきである。承認された以降、実装ステージが始まる。本章では、組織が決定した IT 業務継続戦略の実装のために必要となる、組織、計画、手順に関る推奨項目を提供する。

組織は、訓練や認知プログラムと同様に、IT-BCP に必要な資源、手順、運用を管理すべきである。実装は、その組織の正式な変更管理プロセスに沿ったプロジェクトとして管理し、さらに BCM プロジェクト管理で、可視化と報告の管理を確実にコントロールする。なお、障害検出・対応・災害復旧の構成要素の実装時は、以下を含む関連国際標準を参照すべきである。

- ISO/IEC18043：侵入検知システムの選定と運用
- ISO/IEC27035：障害対応手順
- ISO/IEC24762：災害時復旧サービス

7.1　IT 業務継続戦略要素の実施

(1) 意識、スキル、知識

IT サービスの要素（要員、施設、テクノロジー、データ、プロセス、サプライヤなど）に関する基本的な意識は、事業継続ガバナンスの支援要件や、IT 準備を含むマネジメントシステムを確実にする要素として重要である。従って、組織は次の事項を実施する。

- 継続的な教育や、関係スタッフへの情報提供プログラム・意識普及の効果を評価するプロセスの確立を通じ、意識の立上げ、強化、維持を図る
- スタッフが IT 業務継続の目標達成にどのように貢献するか、認識しているかを確認する

組織は、IT 業務継続マネジメントの役割をアサインされた全ての要員が、要求されタスクの実行に適任であることを、以下によって確認する。

- その要員に必要な能力を見極める
- その要員に必要な訓練の分析の実施
- 訓練の提供
- 必要な能力が達成されたことの確認
- 教育、訓練、スキル、経験、資格に関する記録の維持

ここでは、災害時にその役割を担う担当者に IT-BCP の意識を、どのように認知させ、そのスキルを維持・向上させるかの重要性を強調している。これは、折角 BCP を策定しても、棚に飾っておくだけでは、万一の時に全く機能しないからである。日頃の訓練・演習を通じ、各担当の役割と他の部門との連携を、再認識させることが重要となる。また、訓練・演習を通じ、手順の見直しが必要となった場合、各担当の責任において修正させることが、理解を深める良い契機にもなる。

(2) 施設

IT バックアップシステムとミッション・クリティカルなデータは、同時被災からの影響を避けるために、本番環境から物理的に離すべきである。

戦略を実装する際は、全ての IT 環境の場所に対する考慮が、行なわれるべきである。例えば、可能ならば、訓練または開発用の IT システムは、本番システムから離しておき、災害発生時は、本番サービスにすぐに使えるよう、これらを再構成するといったことも想定される。

全体の拡張性、管理の容易性、サポータビリティ、パフォーマンス そして、実装方法で異なるコスト傾向といった点について、全体の業務継続目的や目標を支えるために選択された戦略を実現するため、最適なテクニックを特定することについて、充分考慮すべきである。

これは、IT 業務継続を経済的・効果的に実現するため、開発用の設備を出来るだけ有効利用するための仕組みである。また、システムを設置する施設についても、システムの分散化が図られた以降は、最上級の施設である必要性は無くなり、あるレベル以上の信頼性を持つ箇所に分散することで、サービスの継続性を維持する、といった考え方も成り立つ。いづれにしても、IT 部門が、全社BCMから要求された RTO を実現するための、方式・構成・施設などを、経済的・効率的に選定することがポイントとなる。

(3) IT テクノロジー戦略

IT テクノロジー戦略としては、以下の実装と調整（ひとつかそれ以上）が想定される。

- ホットスタンバイ: IT インフラが二つのサイト間で複製されている
- ウォームスタンバイ: IT インフラが部分的に準備されている二次サイトで回復作業が行われる
- コールドスタンバイ: 代替場所でスクラッチからインフラが構築され、または構成される
- 出荷合意: 外部サービスプロバイダーによってハードウェアが提供される
- 上記戦略の組み合わせ: 選択と混在の手法

バックアップ用設備は、あくまでも RTO を満足するために設計・構築・運用される。理想は全てをホットスタンバイ構成にすることであるが、コスト面からは到底現実的な戦略とは言えない。

バックアップ用設備はビジネス側が求める RTO を実現するのが目的なので、全ての設備を高いレベルで構成する必要はない。あるシステムはホット、他のシステムはウォームまたはコールドで、ビジネス側が求める RTO を満足さえすれば、最も経済的な構成が理想である。

全社 BCP に則した IT-BCP の仕組みであっても、時間経過とともにビジネス側の要件が変更されることも想定される。その場合は、可能な限り速やかに、そのギャップの解消に取り組むこととし、実装が完了するまでは、それをリスクとしてビジネス側も IT 側も認識しておく必要がある。

(4) データ

データの可用性のための準備は、IT-BCP 管理戦略で定義した要件に沿っていなくてはならない。また、以下の項目を含む。

- 事業継続プログラムで定義された時間内で、可用性を確実にするためのフォーマットで書かれた、データ用の追加記録装置
- データの安全性と機密性を保つ物理的または仮想的なデータ保管のための、代替場所の維

持と、これに必要な適切なアクセス手順の構築。もし情報保管が第三者により提供されている場合、情報管理者は適切な管理万全を期す必要がある

ウォームやコールドスタンバイ方式では、データをそのリカバリ方法と対応した形式で保管する必要がある。データの漏洩や紛失が発生しないよう、その保管、使用については、万全の管理ルールを整備する必要がある。また、データを RTO 以内で回復するために必要な、データ蓄積用（復元用）の設備を、リカバリ・サイトに設置しておく必要がある。

(5) プロセス

IT 業務継続プロセスは、担当者がそれらを実行するため、充分な詳細さと明確さで、文書化されなくてはならない。これは、それら手順が、通常の業務環境で使用する手順と、異なることが想定されるためである。

これらの文書化されたプロセスには、代替場所で、通常の場所と同様の運用を行う手順が含まれる。現実的には、被害の正確な状況（例： 損失やダメージの度合）や、その組織の運用の優先順、外部ステークホルダーの要求などを踏まえ、手順が選定される。

被害状況によっては、最優先のシステムの再開に時間が掛かる一方、次優先順位のシステムの再開が容易という状況も想定される。この場合、実際の再開作業では、対策本部は収集した情報から、各種リソースの状況を踏まえ、どのように業務を再開するのが合理的かつ効率的かを検討し、対策本部（ビジネス側と ICT 側の両者）の判断として、関係者に作業指示する必要も想定される。また、バックアップシステムの操作では、日常の操作と異なるため、留意すべき事項が多々想定される。この点については、手順の中で、担当者が明確に理解出来るよう、記述しておく必要がある。

(6) サプライヤ

組織は、重要なサプライヤが、ビジネス側の要求する IT 業務継続サービス能力を支えることができることを確認すべきである。確認事項には、障害対応と顧客側BCPからの協力要請の同時並行作業をサポートする適切なスタッフと能力、サプライヤ自身で文書化しテストされた IT-BCP、を含む事業継続計画があること、などを含む。

組織は、契約前にサプライヤの人数と能力を評価するプロセスと共に、契約後のサプライヤの可用性を継続的に監視し、見直すプロセスを確立すべきである。要件や関係する規程に対するコンプライアンスは、サプライヤの能力を判断する有効な手段である。例えば、『ISO/IEC24762： 代替実行施設の運営と管理、ICT 災害復旧サービスの提供を行うサプライヤによるベストプラクティス』の採用などである。

重要業務に必須となる関連サービスについては、契約者側として、どのような要件を委託先に求めるについて予め整理、明記し、候補者のレベルを一定水準以上に絞ることが有効となる。また、契約プロセスの中でも、その実効性について、充分に確認・検証することが重要となる。また、契約締結後も、その実効性を維持するため、自社の BCP 訓練への共同参加要請（これも契約条件にすると良い）や、委託先の訓練実施状況の検証などを通じ、委託先の事業継続性を確実にしておくことが重要となる。ここでは、BCP のレベルを検証するための手段として、他の認証規格に対する対応状況、ISO/IEC 27001 や ISO/IEC 20000 など、システム関連の認証の取得状況とその運営状況などを参照することで、委託先のプロセス管理のレベルを推測することが出来るとしている。

7.2 障害対応

いかなる IT 障害に対しても、以下に対する障害対応があるべきである。

- 障害の特質と規模の確認
- 状況のコントロール
- 障害の抑制
- 関係者との連絡

障害対応は、適切な IT-BCP 発動の契機となる。この対応は、組織の BCM 障害対応に統合され、障害管理チーム（IMT）の発動や、また小規模の組織では、障害や事業継続管理に責任がある一人の活動開始となる。

大規模組織では、階層的アプローチを用い、異なる機能に合わせた各々のチームを立ち上げることが想定される。ICT 部門では、技術的またはサービスに関連した事項を基準に、チームを編成する。障害管理の役割は、障害対応の実行、運用、調整、情報伝達に関する計画を策定することである。

7.3 IT-BCP

組織は、潜在的なサービス中断を管理し、それによって IT サービスの継続と重要業務の回復を可能にする計画書を、策定すべきである。

組織の IT 障害管理においては、組織の業務継続と技術的なリカバリ計画は、迅速に継承または同時並行的に実行されることが想定される。組織は、IT サービスを、「通常」状態にもどすための、回復または再開する具体的な計画書（復旧計画）を策定する。しかし、障害から暫くの間は、「通常」がどのようなものか定義することはできないため、ただちにリカバリ計画を実行することはできないことが想定される。組織は、それゆえに、継続に関する計画において、より広い事業継続の支援に運用を拡張できるよう、またリカバリ計画（通常に戻す）の策定のための時間を確保すべきである。

災害発生後、各種情報が集約された結果、計画では最優先に対応しなければならない業務が自社のリソース（ハード、施設、人的など）の問題や外部要因で、予定とおり再開出来ない状況も想定される。この場合、次に優先継続すべき業務の再開が容易に出来るようであれば、まずは出来るところから実施する、といった臨機応変の判断が求められる。ここで「通常」状態について述べているのは、そのような背景を踏まえてである。まずは、社内だけでなく、社外を含めた的確な情報収集と、情報を基にした判断が重要となる。

(1) 計画文書の内容

小規模の組織では、業務全体の IT サービスのすべての回復作業は、ひとつの計画書となることも想定される一方、大規模な組織では、特定の IT サービスの要素を詳細に規定した、多くの計画書を保持することが想定される。

IT 対応やリカバリ計画は、計画で規定された役割に対して簡潔であり、使いやすいものであるべきである。計画書には、以下の要素を含むべきである。

① 目的と範囲

それぞれの計画毎に、その目的と範囲が定義され、トップマネジメントから承認され、その計画を発動に関わる関係者に理解されていること。その組織内の他の関連計画や文書、特に BCP に関し、それらが記述された、計画の入手またはアクセス方法が明確に参照されていること。

各障害管理や IT 対応・リカバリ計画は、以下の観点で優先順位設定に関する考え方を定める。なお、計画には、障害完結後のレビュープロセスで使われる、適切な手順やチェックリストなども含まれていること。

- 回復される重要 IT サービス業務
- 回復されるそれら業務の時間軸
- 各重要 IT サービス業務に必要な回復レベル
- 各計画が発動される状況

② 役割と責任

障害発生中やその過程での、権限のある人やチームの役割と責任（意思決定と支出の権限）は、明確に文書化されるべきである。

③ 計画の発動

早期の障害の封じ込めや拡大防止の機会を失うことよりも、まず IT の事業継続対応を始動し、状況を判断した後にそれを停止するほうが、概ね優れているといえる。従って、組織は、潜在的な IT 関連サービスの中断を管理するための基礎となる、より広い範囲／部門の事業継続の事故管理計画に含まれる、障害管理のエスカレーションと発動手順を、うまく活用する必要があり、IT 対応およびリカバリ計画によって発動される方法は、明確に文書化する。

このプロセスでは、関連する計画またはその一部でも、中断の恐れが見込まれる場合や事故発生直後において、可能な限り短時間に発動することを許容すべきである。計画は、以下について、明確で具体的な記述をすべきである。

- どのように、アサインされた個人やチームを動員するか
- 緊急の集合場所
- 後続のチームの待ち合わせ場所やすべての代替待ち合わせ場所（大組織では、これらの待ち合わせ場所はコマンドセンタとして使われることが想定される）
- 組織が、IT-BCP に基づく対応が必要でないと見なす条件（例、軽微な障害や停電、重要な ICT サービスと見なされるが、通常のヘルプ・デスクや保守対応で管理可能といった場合）

組織は、障害収束後に、IT 対応チームを解散し、通常業務に復帰するためのプロセスを、明確に文書化すべきである。

ここでは、事業継続対応の発動に躊躇している間に、被害が拡大するよりも、まずは対応チームを立上、重大な問題でなければ、速やかにチームを解散するような運営をすべきと強調している。早期の情報収集、状況把握、判断、指示、進捗管理といった流れを、如何に円滑に運営するかがポイントとなる。

④ IT 対応およびリカバリ計画書のオーナーと維持責任者

組織は、IT 対応およびリカバリ計画の文書化に関する、主オーナーを指名し、また文書を定期的にレビュー、改正、更新する責任者を決定し登録すべきである。

バージョン管理のしくみを採用し、変更に関する情報は、正式に継続計画を配布し維持管理されている全ての関係部署に、正式に通知する必要がある。

⑤ 詳細な連絡先情報

連絡先の記録は、「就業時間外」の連絡先を含む。しかし、計画がこのような個人的な内容を参照する場所は、データ保護について充分考慮される必要がある。

7.4 IT-BCP 文書

IT-BCP 文書は、柔軟で、実行可能で、適切であり、読みやすく、理解しやすく、かつ、ビジネス側が IT-BCP 対応の利点とみなした、深刻な事態を管理するための背景説明が明確であることが求められる。文書化は、以下を含めて策定されたリカバリ計画に基づき、包括的な枠組みを定義すべきである。

- 全体戦略
- 重要サービス(RTO/RPO を含む)
- 回復のためのタイムライン
- リカバリ・チームとその責任

IT-BCP 文書は、あるレベルの要員が障害発生時に使うことができるよう、以下を含め、文書化すべきである。

① 目標: 計画の目標の簡潔な記述
② 範囲: BIA の結果を参照しながら、以下を含める
   - サービスの重要性:関連のあるサービスの説明とそれらの重要度の説明
   - テクノロジー:設置場所を含む、サービスをサポートする主なテクノロジーの概要
   - 組織:そのテクノロジーを管理する組織の概要 (部門、主要人物、手続き)
   - 文書:テクノロジーに関する主なドキュメントの概要、保管場所(オフサイトも)を含む
③ 可用性要件:サービスの可用性や関連するテクノロジーに関する業務が定義した要件
④ 情報セキュリティ要件:機密性、正確性、可用性要件を含む、サービス、システム、データに関する情報セキュリティ要件
⑤ テクノロジー的なリカバリ手順:以下を含めた、IT サービス・リカバリのための手順の記述。
   - 作業リスト。 例、デスクトップサポートやコンタクト情報の復元
   - ネットワーク、システム、アプリケーション、データベースなどのリカバリ手順リスト。異なった環境を考慮した、代替場所で再開した場合の合意レベル。(例、回線容量、システム間通信などに影響がある)
   - セキュリティ、ルーティング、ロギングのような、基本的な機能の回復作業リスト

- アプリケーション、またはアプリケーション間、データ同期、情報のバックログ操作のための自動化プロシジャとの調整
- IT サービスの復旧やユーザがリカバリ・モードでの運用に引き継ぐために必要な手順
- バックアップ手順
- 他に情報や指示を得ることができる場所や方法。例、ホットライン番号など
- 通常に戻すステップ

⑥ 添付資料

- 情報システム、アプリケーション、データベースの資産情報
- ネットワーク基盤やサーバ名の概要
- ハードウェアやシステムソフトウェアの資産情報
- 契約やサービスレベル合意

⑦ 主な IT サプライヤ

- 通常のビジネスでのサプライヤ
- リカバリ・サービスサプライヤ

7.5 記録の管理と管理ルール

文書管理は、以下を満たす必要がある。

- 文書を読みやすく、識別可能で検索可能な状態に維持する
- 文書の特定、保管、保護、検索機能の提供

文書の管理ルールは、以下を確実にする必要がある。

- 文書が、課題の前に適切に承認されていること
- 文書が、見直され、必要に応じた修正と再承認がなされていること
- 文書の変更や現在の改正状況が確認されること
- 該当の文書の関連バージョンが、使用するときに使えること
- 外部の元文書が確認され、それらの配布が管理されること

第 8 章　IT-BCP の維持管理

8.1　IT-BCP の保守

IT-BCP の変更には、間違った変更をするリスクや既存のやり方を混乱させるリスクもあるため、IT-BCP の戦略は、柔軟性や適用性が必要とされる。IT サービスの変更は、技術的な面だけでなくビジネス的な観点からも、その変更による事業継続性を評価してから行うこと。

8.1.1 保守活動について

IT-BCM（IT-BCP の維持管理）には、以下が含まれる。

- トップマネジメントによる、BCM 要件と IT-BCP の適応の確認
- IT-BCP 変更管理プロセスの対象範囲に、IT 業務継続戦略の計画・実施に責任があるすべての組織を含むこと
- 新しい IT サービスの開発（更改、改善を含む）プロセスにおいて、レジリエンスの観点で承認されていること
- 統合や合併に際しての、適正評価にレジリエンス評価を含むこと
- IT コンポーネントの廃止を、IT-BCM に反映させること

8.1.2 脅威の監視

緊急のセキュリティ脅威の監視や検出に関する定常的なプロセスを確立すること。この監視プロセス以外にも、以下は IT サービス継続にとって脅威となりうる。

a) 要員のスキルや知識が充分ではなく、オペレーションミスに引き起こす危険がないか
b) IT 設置場所の施設管理は充分でないか （例. コンピュータルームのセキュリティ監視）
c) 利用しているテクノロジー、建物、設備、ネットワークの変更に、IT サービス継続にとって問題がないか。これらの継続利用に問題はないか。
d) アプリケーションとデータベースの変更は適切か、誤った変更による IT サービス中断は考えられないか。
e) IT サービス提供のための、財務、予算は充分確保されているか
f) 外部サービスやサプライヤは安定しており、サービス中断の可能性はないか

8.1.3 テストと訓練

単に、IT サービスの回復だけでなく、以下を確認するための、防御及びレジリエンス要素について訓練する。

a) IT サービスが様々な脅威から守られ、継続され、障害の程度に関係なく回復することができること
b) IT-BCP の対応がビジネスへの影響を最小化できること
c) 被災後、通常ビジネスへの戻り手順が有効であること

8.1.3.1 テスト訓練プログラム

実効性の高い IT-BCP を目指すには、何回かのテストや訓練を繰り返す必要があり、障害全体をシミュレーションする訓練体制が必要である。訓練も、コンピュータルームでの作業から始まり、異なるレベルで、エンド・ツー・エンドでの IT サービス提供における観点を意識したものでなくてはいけない。

テストや訓練に伴うリスクを理解する必要があるが、組織が許容できないリスクレベルまで訓練を広げてはいけない。個々の訓練がどのようにリスクを含んでおり、管理されているかを確認し、トップマネジメントはそれを理解した上で、訓練プログラムを承認するべきである。

テストと訓練は、IT-BCP の具体的な要素を確認するために、ビジネス目標と IT 面での目標の両方が必要である。例えば、次のような項目である。

- ビジネス目標:受注業務を 12 時間以内に再開させる
- IT 目標:受注システムを 8 時間以内に復旧させるために、代替サーバへの切り替えを 2 時間以内、データ回復作業を 4 時間以内、回線切替を 2 時間以内に行う

サーバ、ディスク、回線などのコンポーネントレベルで、別々に訓練することは、全体システム訓練を補完するため、継続的にテストや訓練プログラムで実施されるべきである。

テスト・訓練プログラムでは、テストや訓練の実施頻度、範囲、各訓練の方法の定義が必要である。訓練範囲のハイレベルでの定義は以下のとおりである。

- データ回復: 破損した単一ファイルまたはデータベースの回復
- 単一サーバの回復(完全再構築を含む)
- アプリケーション回復(複数のサーバ、サブプログラム、インフラから構成される)
- 高可用性プラットフォームでのフェールオーバー(クラスタリング装置で、クラスターのペアのひとつが無くなった場合のシミュレーションなど)
- テープからのデータ回復(外部テープ保管場所からの、単一ファイルまたは一連のファイル回復)
- ネットワークテスト
- 通信インフラの切替テスト

訓練は、テストの前提、相互関係、関係するエンドユーザ組織を増やして、前向きに行うこと。

8.1.3.2 訓練の目的

訓練は、以下の目的を達成するために実施する。

- ビジネス要件にあった、IT-BCP であるという組織全体の自信を得る
- IT サービスが、合意された SLA での回復目標内で、維持され回復されること
- IT サービスが、代替ロケーションで事前にテストした状態に復旧されること
- BCM 要員が、回復手順に慣れること
- BCM 要員を教育し、IT-BCP の手順に関する充分な知識を持っていることの確認
- IT-BCP が IT 基盤や他の基盤とズレがないことの確認
- IT-BCP 戦略、IT アーキテクチャまたは回復手順に必要な改善の確認

- 監査証跡や組織のコンプライアンスに必要な情報の提供

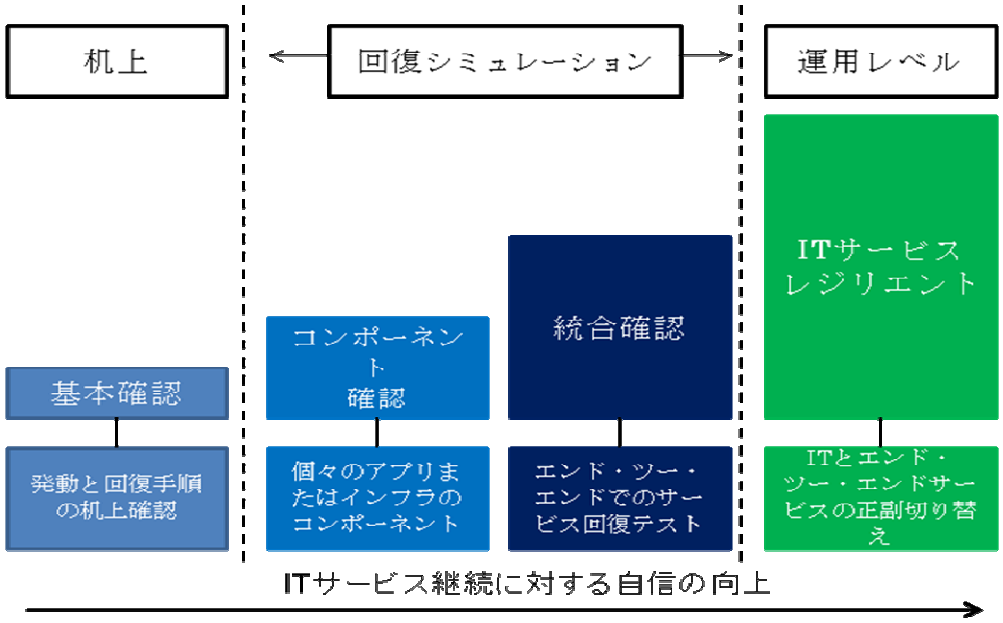
訓練は、コンピュータルームからエンドユーザのデスクトップ PC に至るまでの、あらゆるサービス提供チャネルで、すべてのコンポーネントに対して実施しなくてはいけない。

8.1.3.3 サービス回復の要素

IT サービスの回復に関係するすべての要素を、訓練する必要がある。訓練は、単にサービスの回復や再開にだけ注力するのではなく、システムが持ちこたえる能力（レジリエンス能力）、システム監視、警報管理に関する信頼性も確認する。

コンポーネントレベルから、ロケーション全体のシステムテストまでの訓練を、自信がつきレジリエンスを達成できるまで実施する必要がある。

図表 5 進捗確認と訓練プログラム



以下を確認すること

カテゴリー	テスト・訓練項目
コンピュータルーム	火災・水漏れ検知システム 避難誘導手順 温度、換気、空調のモニターリングテスト 警報プロトコルの訓練
ネットワーク	ネットワーク多様化 ネットワークセキュリティ(アンチウィルス防御や侵入防止、検知)
ハードウェア	故障検知、代替機への切替手順、切戻し手順、修理交換の手配

ソフトウェア	回復手順、
データ	データ回復手順、RPO の達成確認、データの整合性、遠隔地保管データの取寄せ手順
サービス	緊急時の SLA、RTO の確認、ユーザ側の役割、IT サービス停止中の業務継続方法、ユーザ側の復旧手順
サプライヤ	緊急時の連絡方法、役割と対応、SLA

上記項目を組み合わせた形での訓練、例えば、次のようなものである。

- 外部 Web プロバイダーとの接続確認
- システム障害による未反映データの再入力とデータの整合性確認
- デスクトップ PC から代替サーバへのログイン接続 (最新パスワードの確認を含む)
- 代替システムと本番システムとの相違点の確認(アプリ機能制限、利用ユーザ制限など)
- システム復旧後の戻し作業確認

8.1.3.4 訓練計画

訓練によって障害が発生し、IT サービスが停止することがないよう、障害発生を最小化するように慎重に計画する。

- すべてのデータは、事前にバックアップをとられていること
- 本番システムとは、隔離された環境で実施する
- 業務時間外またはユーザが IT サービスを利用していない時に実施する

ステークホルダーと事前に合意し、ビジネスプロセスの中断は最小化されていること。本番で障害が発生中には訓練は実施しない。以下の項目を含む文書を作成する。

図表 6 記述内容と記述例

項目	記述内容	記述例
訓練の記述	訓練の内容や方法を記述する	ディスク障害を想定してデータ回復訓練を実機を使って訓練する
目的	訓練による確認ポイント	バックアップデータが意図されたとおりに回復できること
対象	訓練の対象システム、データ 対象となる部署や要員	データベース回復手順の確認、回復担当者への手順の習熟
前提	訓練に関係のある主な前提	土曜に保管データは取寄せること。当該ディスク以外は正常に稼動とする。
制限	実被災時の状況との違いを記述 時間的な制限	回復日付と実日付は異なる。 日曜の夕方 18 時までに訓練を終了する

リスク	訓練中に発生する可能性がある リスク	データの戻しに時間がかかり、時間内に訓練が終了しない
成功クライテリア	予定している確認項目、結果 パフォーマンス目標 その他	手順を時間内で正しく実施すること。前週末の営業終了時点にデータが戻せること
使用リソース	システム機器、データ、メディア、使用する手順書　など	データベース名、外部保管テープボリューム名等
役割と責任	訓練参加部署、訓練参加要員の役割を記述する	訓練スポンサー、訓練事務局、訓練実施者、問題管理者、 参加ユーザ等
スケジュール	事前計画段階での訓練関係者への説明会、準備作業の日程 訓練前日～当日の詳細なタイムスケジュール、 訓練実施後の報告会までの大まかな日程など	データ準備:10/1(土) 回復前作業:10/1(土) 訓練開始:10/2(日) 9:00 訓練終了:10/2(日)18:00 後処理終了:10/2(日)21:00
必要なデータ	訓練用に必要なデータを記載 訓練用の ID・パスワードなど	9 月最終週に取得したデータを使用。
訓練・障害の記録	記録を取る内容、収集データの記載	障害発生記録、作業の時間経過
訓練終了後の実施項目	訓練内容の確認項目 報告書の作成、報告会に開催などに関する記載。	データの整合性確認作業 訓練終了後 1 週間以内に報告書を作成、2 週間後を目処に報告会を開催する

8.1.3.5 訓練の管理

役割と責任を付与された適任者が、訓練を指揮するための体制を構築するには、以下の項目を実施すること。

① 指揮方法の確認

どのように訓練を進めるか、指示の伝達方法や使用するツール（電話、FAXなど、実際の被災時に使用するもの）、コマンドルームの設置と必要な機器・備品の確認を行う。

② 意思伝達の確認

一斉連絡、担当者への指示など指揮者からの伝達だけでなく、担当者からの連絡や報告を含む意思伝達方法を確認する。伝達する相手、内容、手段を確認する。

③ 訓練スタッフの確保

安全に訓練を実施するために必要な要員を確保する。訓練と並行して本番システム運用が行われている場合は、本番への影響がないよう人選には注意する。特に、代替センターへの移動を伴う場合は、訓練中に本番システムで問題が発生した場合に対処できるよう考慮する。

④ オブザーバ、ファシリテータの確保

訓練の進捗状況、スケジュール管理、発生した問題を記録する要員を確保する。客観的な評価を必要とする場合は、BCM 要員以外の外部の人員を検討し、育成目的で BCM 要員候補のアサインを検討する。

⑤ 訓練マイルストーンの確認

時間軸に合わせた主なチェックポイントを設定する。マイルストーンは想定される作業結果と実施時刻からなり、予定と実績の比較は、訓練の評価にも使用する。

⑥ 訓練終了手順の確認

訓練終了後の後作業を確認する。通常業務が再開可能な環境へ戻ったことを確認する手順、訓練データの消去、本番データのリストア、システム切戻し確認(切替を行った場合)、ネットワーク接続確認、訓練事務局の設営解除作業など。

⑦ 訓練停止手順

本番システムでトラブルが発生した場合、作業予定時間を超過した場合など、緊急事態が発生した場合に、訓練を途中で打ち切るための手順を確認する。

8.1.3.6 レビュー

訓練結果のフォローのために、以下を実施する。

① 訓練結果からの気づきの確認

訓練参加者からのアンケートやディスカッション等により、気づいた点を取りまとめる。改善点だけでなく、想定外の判断や良かった点、訓練によって学んだ点なども収集する。

② 訓練目標と成功クライテリアの確認

訓練目標の達成状況を確認する。成功クライテリアの設定が正しかったか、目標は達成できたか、できなかった場合は原因を話し合う。

③ 想定された時間内での実施項目と割り振りに関する確認

時間内での作業項目は妥当か、要員人数が十分か、作業の順番や並行作業の可否などを確認する。

④ ギャップの確認

IT-BCP で検討された、プロセス、手順、システムリソース、要員のスキルおよび人数、使用機器など、訓練で想定した被災への対策での、過不足を確認する。1，2で検討された内容からの改善点

を抽出する。

例 1） 初動対応の人数が足りなかった。

例 2） テープ装置台数が足りず、データリストアに時間がかかった。

⑤ 訓練スポンサーから考察と訓練レポートの作成

訓練スポンサーからの講評。ビジネス視点、マネジメント視点での考察をまとめる。監査や上位マネジメント向けの訓練レポートを作成する。

⑥ 各アクションプランの統合とフォローアップ

各担当者から出されたアクションプラン(要対応事項)を統合し、対応に関する進捗管理を行う。

8.2 IT-BCP 内部監査

IT 業務継続内部監査計画には、監査基準、監査範囲、監査実施頻度、監査方法を記載する。例えば、IT 業務継続内部監査は、年次で行うなど。

内部監査人が監査計画を確認し、監査人の選定および監査実施は、客観性と公平性のある手順で実施しなくてはいけない。監査人は、監査人教育を受講するなど、必要なスキルや知識を持っていること。

IT 業務継続内部監査によって指摘された改善事項を確実に実行するための手順を確立すること。例えば、部署の重点実施項目に入れるなど。

監査には外部監査も含まれること。アウトソーシングベンダは、通常運用や災害時対策に関して、IT-BCP の実効性を監査されなくてはならない。IT-BCP の監査結果は、文書化され報告されること。マネジメントは、監査結果とフォローアップ項目の実施状況をレビューすること。

8.3 マネジメントレビュー

トップマネジメントは、内部監査、外部監査または自己評価により、BCM がきちんと稼働していることを確認し、IT 業務継続ポリシーおよび目標、IT 業務継続マネジメントに関する改善や変更を評価する。

年次で以下を見直し、結果は文書化されること。

- IT-BCP 要件
- ICT サービス
- 重要 ICT サービスリスト
- 重要 ICT の現状と事業継続要件とのギャップにもとづくリスク

8.3.1 マネジメントへのインプット

マネジメントレビューへのインプット情報は以下のとおり。

a） 内部サービスレベル

b） 外部サービスプロバイダーの SLA 維持能力

c) 監査結果
d) 関係団体からのコメント、独自見解を含む
e) 予算措置及び改善措置の状況
f) 残存リスクと許容リスクのレベル
g) 前回のマネジメントレビューからのフォローアップ項目
h) テスト、訓練、障害からの学びと教育啓蒙プログラム
i) 新しい実践とガイドライン

8.3.2 レビューからのアウトプット

トップマネジメントが署名するレビュー成果物には、以下を含むこと。

a) IT 業務継続マネジメントシステムの管理対象を広げるべきかどうかの検討結果
b) IT 業務継続マネジメントシステムをより効果的に運用するための改善点
c) ICT サービス定義、重要 ICT サービスリスト、IT-BCP 要件の差し替え、IT-BCP の対応レベルと事業継続要件のギャップに伴うリスクに関する記述
d) IT 業務継続対策、手順の修正。必要に応じて ICT サービスに影響がある内的・外的事象への要対応項目
e) IT-BCP の実践及び維持管理に必要なリソースの要求。要員の増員、システム資源など
f) IT-BCP の実践及び維持管理に必要な財務及び予算に関する要求

8.4 IT サービスのパフォーマンス評価

IT 対応能力を、所定のパフォーマンスクライテリアで評価するプロセスを実施する。また、IT-BCP の評価は、定量的または定性的であること。

8.4.1 定量的な評価項目

監視データの収集は、本番システムへ影響のない範囲で行うこと。

- IT サービス中断の前に検知されなかった障害の数： 検知時間の遅れの発生。アラートメカニズムを改善につながる
- 障害の検知にかかった時間： アラートから実際に障害を認知するまでにかかった時間
- 影響のない障害の通知数： 影響のない通知数の割合
- イベント監視で収集したデータの利用： 障害分析などのためにデータが有効利用されているか。有効なデータが収集されているか

8.4.2 定性的な評価項目

IT-BCP の計画、準備、実行における手順の有効性を、以下の方法で確認する。

- 質問による調査
- BCM 担当者やステークホルダーからのフィードバック
- 意見交換のためのワークショップ開催
- グループ会議

第 9 章　IT-BCP の改善

IT-BCP を継続的に改善するためには、その組織での BIA や選定されたリスクによって定められた潜在的なインパクトに適した改善策や予防策を行う。

9.1　改善策

IT サービスの中断を改善していくには、以下の要件を定義すること。

- 中断の定義
- 中断原因の特定
- トラブルが繰り返されないような必要な対策の評価
- 改善策の確認と実施
- 実施された対策の結果の記録
- 改善策のレビュー

9.2　予防策

IT-BCP 要素の脆弱性を確認し、以下を実施するための手順を文書化する。

- 潜在的なトラブル発生の特定
  例） システム更改、アプリケーション変更、担当者の交代、業務ピーク時間帯などトラブルが発生しやすいタイミングを記述する。
- 中断の原因の特定する手順
  例） 直前に実施した変更の確認、システムデータの解析手順など
- 必要な予防策の決定と実施に関する手順
  例）システムリリース判定項目、リリース手順、フォールバック手順など
- 実施された対策の結果を記録しレビューする手順
  例） システム変更のリリース前に実施すべきテスト項目とテスト結果のレビュー

【参考文献】

1) 『IT サービス継続ガイドライン』 経済産業省、2008 年 9 月
2) 『ISO/IEC 20000 活用ガイドと実践事例』、ISO/IEC 20000 活用ガイドと実践事例編集委員会編著（編集委員長 大畑毅）、日本規格協会、2008 年 1 月 28 日
3) 『ISO/IEC 17799:2005 情報セキュリティマネジメントの実践のための規範』、中尾康二・中野初美・平野芳行・吉田健一郎 共著、日本規格協会、2007 年 3 月 8 日
4) 『BS 25777:2008 Information and communications technology continuity management - Code of practice』、British Standard Institution、2008 年 11 月

IT サービス業務継続ガイドライン
- ビジネス継続を支える IT サービス提供のために -

2011 年 3 月 18 日　Version 1　発表　©

著　者:　深谷純子　深谷レジリエンス研究所
伊藤　繁　株式会社野村総合研究所
田代邦幸　株式会社インターリスク総研
黄野吉博　社団法人日本工業技術振興協会

発　行:　レジリエンス協議会　ICT チーム
〒105-0003　東京都港区西新橋 1-5-5　社団法人日本工業振興協会内
電話　03-3597-7888