事業継続のための

高回復力システム基盤導入ガイド

概　要　編

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

C O N T E N T S

はじめに

2011 年 3 月 11 日の東日本大震災では、多くの人の命が失われるとともに、社会基盤や企業も甚大な被害を受けました。社会や企業などを支える情報通信や情報システムの停止、データの喪失などにより長期にわたって業務が中断された地方公共団体や企業もありました。

被災企業などの中には、事前に検討した災害対策や被災時の対応手順などが有効に機能した事例もありましたが、一部を除いては、十分な情報システムの災害対策や被災時の対応手順などが整備されていませんでした。震災をきっかけに事業継続への意識は高まっていますが、未だ具体的な対策の着手に至っていない組織も少なくないのが現状です。

また、近年、企業などの情報システムに大規模なシステム障害が発生し、長時間に渡って他の組織や消費者に対するサービスを中断しなければならない事象が散見されています。ネットビジネスの増加やサプライチェーンの高度化など、情報システムの停止が即、業務やサービスの中断に繋がるようなケースも増えています。このことは、災害だけではなく、大規模障害についても未だ十分な備えができていないことを示しています。

これらは、情報システムの災害対策や障害対策への投資について経営層の理解が十分に得られていないこと、また、災害や障害の対策、対応手順などの整備の前提となる被害想定やそれに基づく事業継続戦略を決定するための考え方や作業などが複雑で、手間のかかることが大きな理由の一部であると考えられます。

一方で、東日本大震災では、被災して情報システムを利用できなくなった組織が、ベンダなどが提供するクラウドサービスなどを利用して業務を再開した事例もみられました。また、これまで遠隔地にバックアップデータの保管を行っていなかったり、災害時の情報システムのバックアップサイトを保有していなかったりした組織が、震災をきっかけとしてクラウドサービスなどをバックアップデータの保管先やバックアップサイトなどに活用しようとする動きも出つつあります。

このような状況を踏まえ、独立行政法人情報処理推進機構の技術本部ソフトウエア・エンジニアリング・センターでは、事業継続戦略の策定やそれを実現する情報システム対策が十分にできていない企業や地方公共団体などが「大規模災害」および「大規模システム障害」に備えた対応を容易に実施できるための「高回復力システム基盤導入ガイド」（以下、「導入ガイド」とします。）を策定するに至りました。導入ガイドでは、これまで費用や専門的スキルをもった要員不足などが理由で、高回復力システム基盤の導入が難しかった組織において、クラウドサービスがその解決策の一つになりうると考え、クラウドサービスを活用した高回復力システム基盤の導入事例なども提供しています。

1．導入ガイドの概要

1.1．導入ガイドの目的と想定する読者

大規模災害や大規模システム障害によって中断した事業活動を迅速に再開するうえで、情報システムの復旧は優先度の高い事項のひとつです。そのためには、災害や障害に強く、万が一停止した場合にも迅速に復旧できるシステム基盤を導入することが不可欠です。導入ガイドでは、このようなシステム基盤を高回復力システム基盤と呼んでいます。

システム基盤とは、業務アプリケーションに対して共通のサービスを提供する仕掛けのことで、ハードウェア機器やネットワーク機器、OS やミドルウェア、更にはその制御や運用のアプリケーションなどの組合せで実現されます[1]。

導入ガイドでは、高回復力システム基盤の導入において上記のシステム基盤を構成する各要素に求められる要件を示しています。なお、導入ガイドでは、業務を再開させるための情報システムの復旧において欠くことができない建物や設備、業務アプリケーションや業務データ、および要員体制なども、高回復システム基盤を構成する要素として取り扱っています。

高回復力システム基盤の導入には、多大な労力を要するとともに、豊富な経験が必要になります。導入ガイドは、高回復力システム基盤に求められる目標復旧時間や強度に応じて分類された 4 つのパターン（以下、「モデルシステム」といいます。）を用いて、より簡易に高回復力システム基盤を導入するための手順や実践的な手法を提供することを目的としています。

導入ガイドが想定する読者は、事業継続のための情報システム対策に未着手、もしくは対策が不十分と考えている組織の経営層、事業部門、および情報システム部門の方々です。

すでに事業継続のための情報システム対策に取り組み、十分な対策を実施していると考えている組織においても、後述する計画編や事例編に示した高回復力システム基盤に必要な要件や対策例などを参照し、現在、実施している対策の網羅性の確認や継続的な改善に活用していただけるものと考えています。

---

[1] 非機能要求グレード利用ガイド［解説編］（独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター）から引用

1．2．導入ガイドの構成と活用方法

導入ガイドは、以下の文書から構成されています（表 1.2-1）。

■表 1.2-1　高回復力システム基盤導入ガイドの構成文書

No	文書名	公開日	本書における略称
1	高回復力システム基盤 導入ガイド（概要編）	2012 年5月	概要編
2	高回復力システム基盤 導入ガイド（計画編）	2012 年5月	計画編
3	高回復力システム基盤 導入ガイド（事例編）	2012 年 6 月（予定）	事例編

概要編は、高回復力システム基盤の必要性や導入方法の概要を紹介するとともに、導入ガイドの特徴である高回復力システム基盤のモデルシステムについて説明しています。

経営層や事業部門には、主に概要編を読んで、高回復力システム基盤導入の必要性を理解していただきたいと思います。また、高回復力システム基盤導入の手順の概要や導入のキーとなるモデルシステムについて理解していただき、実際の導入において必要な意思決定などを行っていただきたいと思います。実際に導入を行う情報システム部門にとっても、概要編は高回復力システム基盤導入の全体像を理解するのに役立ちます。

計画編は、モデルシステムを活用して、高回復力システム基盤を導入する際の詳しい手順や内容について説明しています。

情報システム部門は、計画編を参照して検討対象となるシステム基盤を選定したり、モデルシステムを活用して導入対象のシステム基盤の要件を確定したりすることができます。なお、モデルシステムの選定においては、経営層の方々や事業部門の関与が必要です。情報システム部門は、計画編に記述されている必要な準備を行って経営層や事業部門の判断を仰いでください。

事例編は、高回復力システム基盤の具体的な導入事例や導入の際のポイントなどを説明しています。

情報システム部門が導入計画に沿って高回復力システム基盤を導入する際には、事例編で提供するモデルシステムごとの導入事例を参照して、具体的な対策手段や活用可能なベンダのサービスなどを検討できます。また、経営層や事業部門は、事例編で紹介される他社での高回復システム基盤導入の背景や実際の状況を参照することによって、モデルシステムの選定時の参考にすることができます。

1.3. 導入ガイドで対象とするリスク

地震、台風、火事などの災害に加え、近年では新型インフルエンザなど、組織の事業継続に対する脅威は数多くあります。このような脅威は、情報システムの稼働に必要な建物、設備、機器をはじめ要員などにも直接的な影響を及ぼし、情報システムを停止させる要因になります。

一方、事業活動のＩＴへの依存度の高まりから、大規模なシステム障害やサイバーテロなどをはじめとした情報セキュリティ事故が原因で、業務の中断が発生している事例が多く見受けられるようになりました。

このような情報システムの停止につながる数多くの脅威のうち、導入ガイドでは、災害とシステム障害を対象としています。特に近年懸念される大規模災害および情報システムが長時間に渡って停止するような大規模なシステム障害を想定しています。

導入ガイドでは、脅威の発生によって引き起こされる情報システムの被害の状況をリスク事象と呼びます。

導入ガイドで対象とするリスク事象は表 1.3-1 のとおりです。

■表 1.3-1　導入ガイドで対象とする脅威とリスク事象

脅威		リスク事象
大規模災害	地震 水害 火災　など	社会インフラ、建物、設備、機器、要員などが被災し、通常使用している情報処理施設での情報システムの提供が長期間できない状態
大規模システム障害	ハードウェア障害 ネットワーク障害 など	ハードウェアの故障やネットワークの切断が発生し、通常使用しているハードウェアやネットワークでの情報システムの提供が長時間できない状態

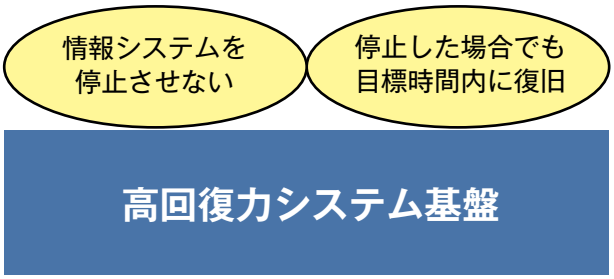
不正アクセスやソフトウェア障害、操作ミスなどの脅威も情報システムの停止につながる重要な脅威ですが、導入ガイドの対象からは外しています。これは、情報セキュリティやソフトウェア障害などの対策が、主に設備や機器などの冗長化を柱とした災害やシステム障害の対策と大きく異なるためです。情報セキュリティ事故やソフトウェア障害を原因とする情報システムの停止については別途、ソフトウェア開発時の品質管理、および事故や障害の発生を迅速に発見し、是正するための仕組みなどを検討することがより重要になります。

2．事業継続のための高回復力システム基盤

2．1．高回復力システム基盤とは

組織の事業継続のための情報システム対策では、情報システムを停止させないための対策と、万が一情報システムが停止してしまった場合に迅速に復旧するための事前準備の両方が重要です。

高回復システム基盤とは、大規模災害や大規模システム障害に対して一定の強度（情報システムを停止させないための対策が施されていること）をもち、万が一停止した場合でも、目標とする時間内に情報システムを復旧することができるように設計・構築されたシステム基盤をいいます（図 2.1-1）。



■図 2.1-1　高回復力システム基盤

導入ガイドでは、システム基盤について、その構成要素ごとに想定されるリスク事象とそれに対応するための基本的な考え方を定めています（表 2.1-1）。また、計画編では、この基本的な考え方に沿ってモデルシステムごとの具体的な要件を示しています。

高回復力システム基盤の要件とは、各モデルシステムが示す目標復旧時間などを達成するためにシステム基盤の各構成要素に求められる要求事項です。例えば、機器やネットワークなどの冗長化の必要性、バックアップデータの取得や保管の方式、運用保守に関する取り決め事項などが該当します。

導入ガイドでは、システム基盤に求められる強度や復旧時間に応じた高回復力システム基盤の４つのモデルシステムを示し、各モデルシステムに必要となる要件を提供しています。なお、モデルシステムの詳細については、「2.3. 高回復力システム基盤のモデルシステム」で説明します。

■表 2.1-1　高回復力システム基盤導入の基本的な考え方

構成要素	リスク事象	基本的な考え方
電源供給・ネットワークサービス	電力、通信、水道などライフラインが長時間利用不能となる。	必要に応じて自家発電装置や貯水槽の設置、ライフライン供給経路の冗長化を図る。
建物、設備	建物や設備など情報処理環境・基盤が損傷し、長時間利用不能となる。	最低限として震度６弱の地震に対する耐震性を確保する。６強以上の地震が想定される地域においては、必要とされる復旧時間などを考慮して、遠隔地にバックアップサイトを確保することを検討する。 想定されるその他の自然災害などについても必要な対策を行う。
ハードウェア機器やネットワーク機器	ハードウェアが損傷し、長時間利用不能となる。	ハードウェアの損傷、故障に備え、必要な範囲で代替機を持つ。大規模災害への対応として、普段使用している情報処理施設とは別の施設を確保する。
ＯＳやミドルウェア	ハードディスクなどの損傷によりソフトウェアが消失し、長時間利用不能となる。	情報システムが復旧したときに、ＯＳ、ミドルウェアを必要な状態で利用できるよう、バックアップを行う。大規模災害への備えとして、遠隔地に保管する。
システム運用の体制や仕組み	情報システムを運用する人材やスキルが不足する。 復旧対応の手順において間違いが起こる。	大規模災害や大規模システム障害時に必要な要員が確保できるように計画を策定する。 復旧対応に必要な手順などの文書化や、訓練を行う。
ハードディスクなどに格納された業務アプリケーション・業務データ	ハードディスクなどの損傷により業務アプリケーションや業務データが消失し、長時間利用不能となる。	情報システムが復旧したときに、業務アプリケーションや業務データを必要な状態で利用できるよう、バックアップを行う。大規模災害への備えとして、遠隔地に保管する。

2.2. 事業継続戦略と情報システムの復旧目標

大規模災害や大規模システム障害により情報システムが停止した場合には、事業継続戦略に沿って情報システムを復旧することが必要です。

事業継続戦略では、災害などによって業務が中断した時点から、いつまでに（業務の目標復旧時間）、どの程度（業務の目標復旧レベル）で再開させるか、また、業務の再開に必要な機器や人が不足する場合、どの業務を優先させるか（業務の復旧優先度）を決定する必要があります。

例えば、「製品の生産再開までの時間を 3 日間（業務の目標復旧時間）、ただし、当初は平常時の 50%の操業（業務の目標復旧レベル）を目標とする。」 また、「生産は、災害時に需要が予想される A 製品を優先（業務の復旧優先度）する。」 といったものが事業継続戦略にあたります。

情報システム部門は、上記の事業継続戦略に沿った業務の再開を実現するために、次のような観点で情報システムの復旧を行う必要があります。

①情報システムの目標復旧時間と復旧優先度

情報システムの復旧から業務を再開するまでに必要な作業時間などを考慮して、情報システムの目標復旧時間を決めます。利用できるシステム基盤のリソース（サーバなどの数や処理能力）が限定される場合には、業務の復旧の優先度に応じた情報システムの復旧優先度を決めておく必要があります。

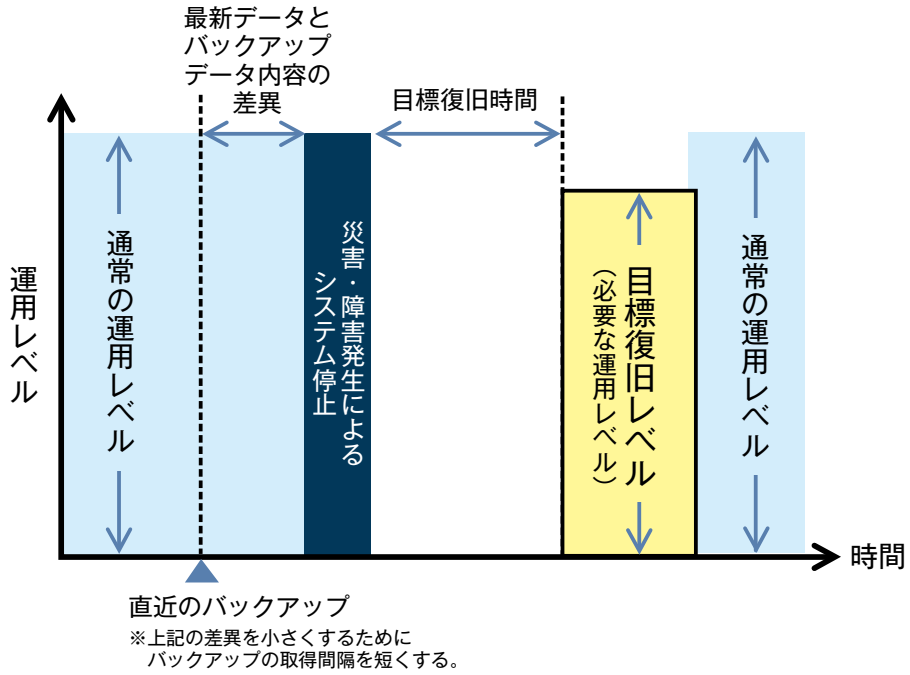
②情報システムの目標復旧レベル

災害などで、通常使用している情報処理施設（以下、「メインサイト」といいます。）が被災し、使用できなくなる場合のために代替施設（以下、「バックアップサイト」といいます）を準備して情報システムを稼働させなければならない場合があります。この場合、バックアップサイトのコストを抑えるために、バックアップサイトの処理能力をメインサイトよりも落とすことがあります。例えば、災害などの非常時において、業務の目標復旧レベルが 50%でもよい場合には、バックアップサイトの情報システムの目標復旧レベルは 50%でよいことになります。

③データのバックアップ取得間隔

情報システムの復旧には、機器やソフトウェアなどに加えて、顧客情報や取引結果などのデータが必要になります。災害や障害などでデータが消失する場合に備えて、バックアップをとっておくことが必要です。しかし、バックアップはあくまでも過去のデータであり、最新の内容とは差異があります。バックアップシステムや代替機などを利用して情報システムを復旧する場合には、この差異を埋めるための作業が必要になります。この作業に必要な時間は直近のバックアップがいつ取得されているかにより決まります。できるだけバックアップデータと最新のデータの内容を近づけるためにはバックアップの取得間隔を短くする必要があります。しかし、バックアップの取得間隔を短くすると情報システムの運用に影響を与えたり、バックアップのコストが高くなったりするため、情報システムの目標復旧時間に合わせて、バックアップの取得間隔を決める必要があります。

以上のことを時系列に沿った図にまとめると、以下のようになります（図 2.2-1）。



■図 2.2-1　情報システムの段階的な回復の概念図

２．３．高回復力システム基盤のモデルシステム

事業継続のための情報システム対策の取り組みにおいては、災害や障害が発生した場合の被害想定や事業への影響度分析を行い、事業継続戦略を決定して、それを実現するためにどのようなシステム基盤が必要かを検討するという手順を踏みます。しかし、事業部門で事業継続戦略を決めてくれない、そもそも被害想定や影響度分析、事業継続戦略の決定の方法がわからない、といったケースも少なくありません。

導入ガイドでは、高回復力システム基盤のモデルシステムを用意し、経営層や事業部門がモデルシステムの選定を通じて、組織の重要な業務に対してどのようなシステム基盤が必要かを判断することができるようにしました。

モデルシステムは、高回復力システム基盤のカタログのようなものです。例えば、自動車の詳しい仕組みは知らなくても、カタログで自動車の性能や装備と、価格を比較して欲しい自動車を選択できるように、ＩＴに詳しくない方でもモデルシステムを参照して自らの組織の要望に適合するシステム基盤を選択することができます。

用意したモデルシステムは、４パターンです。それぞれのモデルシステムは、以下の点で特徴づけられます。

① 必要となるシステム基盤の強度（災害や障害への耐性）
② 情報システムの復旧にかかる時間
③ 高回復力システム基盤導入のための投資規模

上記のモデルシステムごとの特徴に大きな影響を与えるシステム基盤の主要な要件は以下のとおりです。

① データのバックアップ方式や取得間隔
② 情報システムを構成する機器やネットワークの冗長化の有無
③ メインサイト被災時用のバックアップサイトの有無

表 2.3-1 にモデルシステムの特徴と主要要件を示します。

■表 2.3-1　モデルシステムの特徴と主要要件

			モデルシステム			
			1	2	3	4
モデルシステムの特徴	①システム基盤の強度		低	中	高	高
	②復旧時間	障害時	1～3日	2時間以内	2時間以内	2時間以内
		災害時	1～6ヶ月	1～6ヶ月	1～7日	2時間以内
	③投資規模		低	中	高	高
モデルシステムの主要要件	①バックアップ方式、取得間隔		非同期 月次	非同期 週次	非同期 数回 / 日	同期 数回 / 時
	②機器などの冗長化		なし	あり	あり	あり
	③バックアップサイト		なし	なし	あり	あり （ホットスタンバイ）

2.4. モデルシステムの要件

ここでは、モデルシステムの要件を説明します。要件は、すべてのモデルシステムで共通のものと、モデルシステムごとに異なるものに分けられます。

すべてのモデルシステムは、以下の共通要件を満たしています。

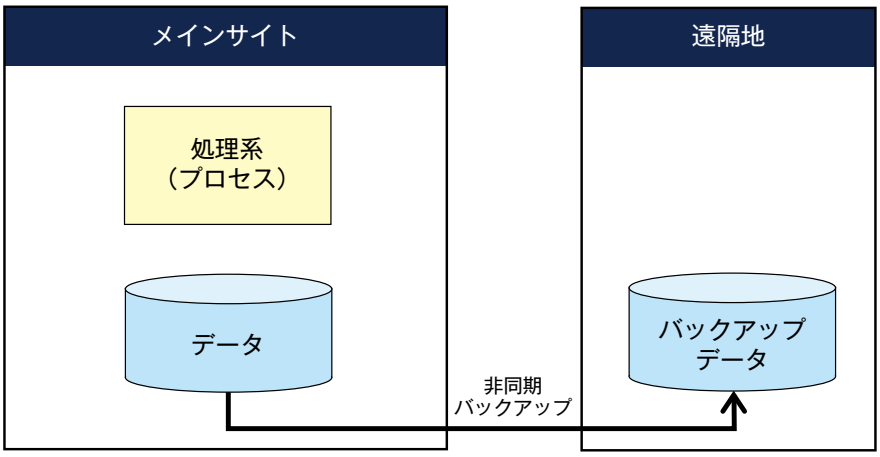
1）建物･設備は、一定の災害規模（地震の場合は少なくとも震度６弱）まで耐えられる。
※導入ガイドでは、震度６強以上の地震の場合、メインサイトの情報システムは停止し、バックアップサイトで業務を継続することを想定しています。実際には、メインサイトの耐震強度の増強などの対策もありえますが、サイトを運営するために必要な電力などのライフラインや要員の確保を考えるとバックアップサイトで業務を継続させることを検討しておくべきです。

2）機器の主要構成要素（CPU、メモリ、ディスク）、電源、通信網は、一定の冗長化が図られている。
※その他、建築基準法、消防法などの法令に加え各地方自治体などが定める条例などにも適合しているものとします。また、洪水など、地域に特有の気象、地理条件などによってリスクが高いと判断した事象にも一定の対策が施されているものとします。

図 2.4-1 ～図 2.4-4 にモデルシステムごとに異なる主要な要件を示します。

モデルシステム１

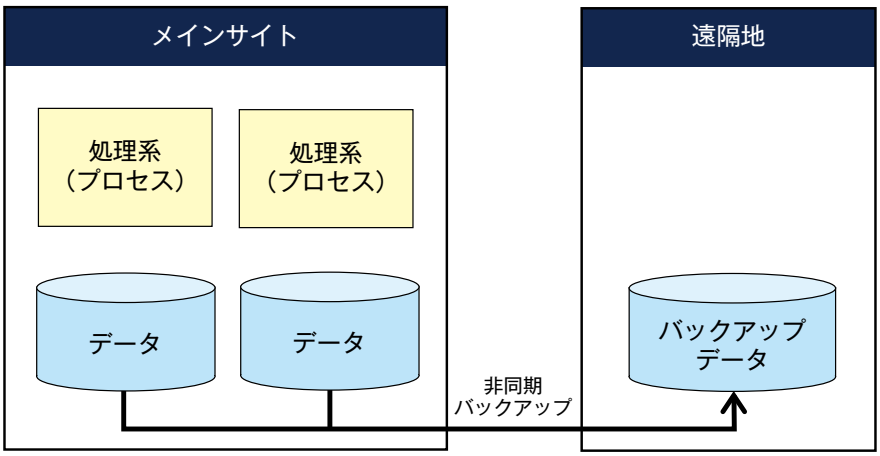
共通要件をベースとした構成。メインサイトの処理は一系統のみで、データなどのバックアップは、遠隔地に保管する。バックアップ方式はオンラインまたはオフライン（定期的に遠隔地に配送）のいずれでも可。



■図 2.4-1　モデルシステム１

モデルシステム２

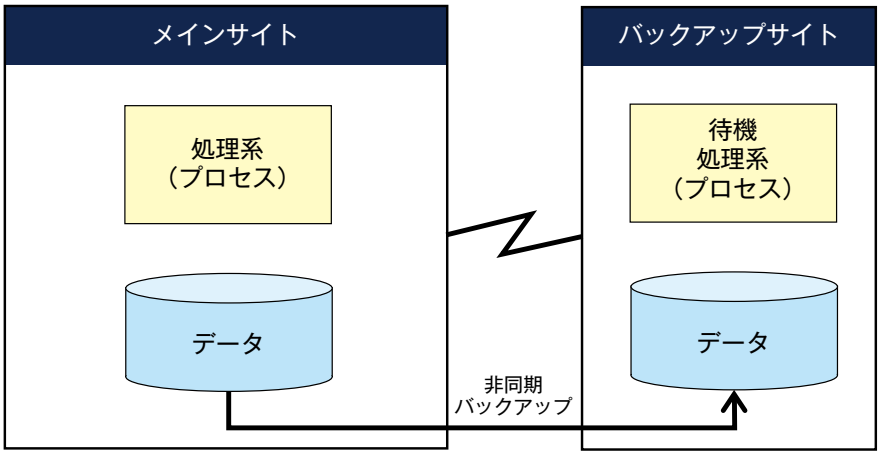
共通要件に加え、メインサイトの処理系を二重化する。通常は両方の処理系で負荷分散し、一方が停止した場合にもう一方のみで稼働するケースと、通常は一方だけが稼働し、停止時に待機している処理系に切り替えるケースがある。バックアップ方式はオンラインまたはオフライン（定期的に遠隔地に配送）のいずれでも可。



■図 2.4-2　モデルシステム２

モデルシステム３

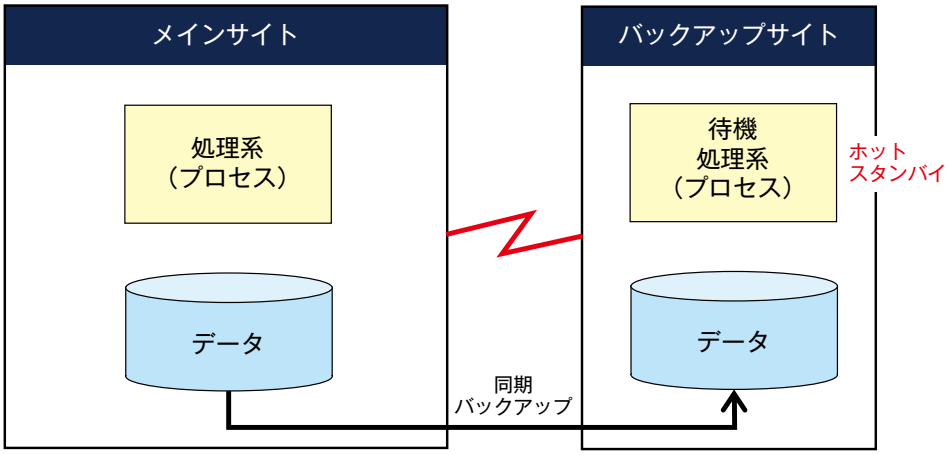
共通要件に加え、バックアップサイトを保有。メインサイトが使用不能になった場合に、バックアップサイトに切り替える。システム障害での長時間停止を防ぐためにメインサイトの処理系を二重化することが多い。バックアップ方式は、オンラインが望ましいが、バックアップの取得間隔によってはオフラインも可。



■図 2.4-3　モデルシステム３

モデルシステム４

共通要件に加え、ホットスタンバイのバックアップサイトを保有。メインサイトが使用不能になった場合に、バックアップサイトに切り替える。通常はメインサイトとバックアップサイトで負荷を分散し、一方が使用不能な場合にもう一方のみで処理を行うケースもある。システム障害での長時間停止を防ぐためにメインサイトの処理系を二重化することが多い。バックアップの取得間隔が短いためバックアップの方式はオンラインとなる。



■図 2.4-4　モデルシステム４

3．高回復力システム基盤の導入

3．1．高回復力システム基盤導入時の経営層の責任

高回復力システム基盤の導入は、経営戦略や事業継続戦略に基づいた事業上の優先順位に基づき実施されるべきものです。そのためには、経営層をはじめ関係者全員の協力と調整が必要です。情報システムが停止しないための予防的な対策や災害・障害発生時の事前準備は、通常の業務運営に不可欠な投資とみなされないことも多いため、組織全体でその必要性が理解されるように経営層の積極的な関与が必要です。

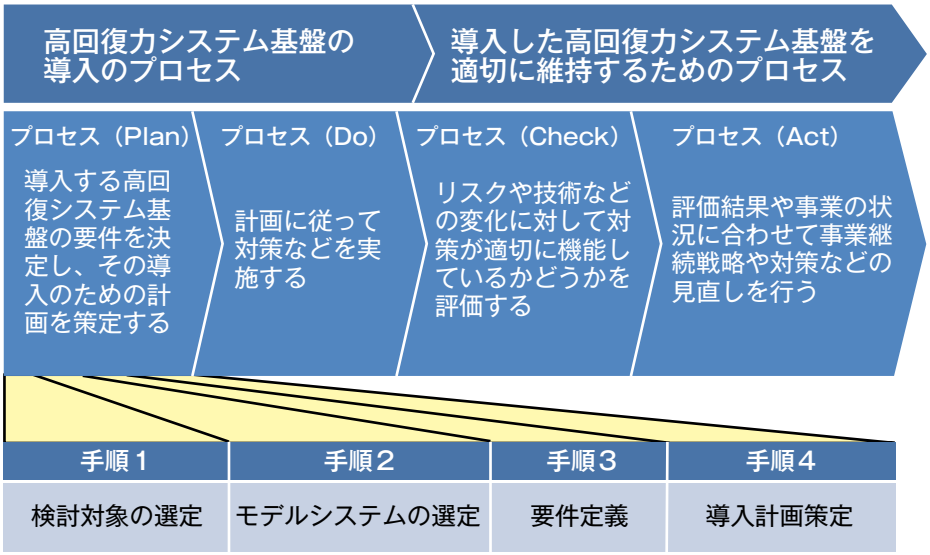
経営層は、高回復力システム基盤の導入に際して、業務の目標復旧時間などの事業継続戦略や投資規模などについて明確な方針を示し、自らも主体的に参画する必要があります。導入ガイドを使用した高回復力システム基盤の導入では、経営層がモデルシステムを選定することによって、組織に必要な事業継続戦略や投資方針を示すことができます。

3.2. 高回復力システム基盤の導入手順

高回復力システム基盤の導入のプロセスは、導入する高回復システム基盤の要件を決定し、その導入のための計画を策定するプロセス（Plan）、計画に従って対策などを実施するプロセス（Do）に分けることができます。また、導入した高回復力システム基盤を適切に維持するためには、リスクや技術などの変化に対して対策が適切に機能しているかどうかを評価するプロセス（Check）、評価結果や事業の状況に合わせて事業継続戦略や対策などの見直しを行うプロセス（Act）も重要です。

導入ガイドでは、導入プロセスのうち「Plan」に該当する部分を紹介します。具体的には、組織の状況に適した高回復力システム基盤の要件を確定し、導入計画を策定するまでを４つの手順に分けて紹介します（図 3.2-1）。

なお、経済産業省から発行されている『ＩＴサービス継続ガイドライン』では、ＩＴサービス継続マネジメントの計画、実行、評価、改善までの一連の手順や管理項目が紹介されています。これらは、高回復力システム基盤の導入、維持管理にも応用可能であり、ご一読されることをお勧めします。



■図 3.2-1　高回復力システム基盤導入手順

導入計画策定のための各手順の実施概要は以下のとおりです。

手順１　検討対象の選定

高回復力システム基盤の適用範囲を特定します。業務の重要性などに応じて対象とする業務システムやこれらに係わるシステム基盤を選定します。

手順２　モデルシステムの選定

手順１で選定したシステム基盤について、適切な高回復力システム基盤のモデルを４つのモデルシステムから選択します。

手順３　要件定義

選択したモデルシステムが提供する要件を参照し、必要な調整を加えて、導入する高回復力システム基盤の要件を確定します。

手順４　導入計画策定

手順３で定義した要件に基づく高回復力システム基盤を導入するための計画を策定します。

表 3.2-1 では、各導入手順での関係者の役割を示します。なお、実際の導入に際しては、企画部門などの他部門が参加し、役割を担う場合もあります。

■表 3.2-1　導入手順の各関係部門の役割

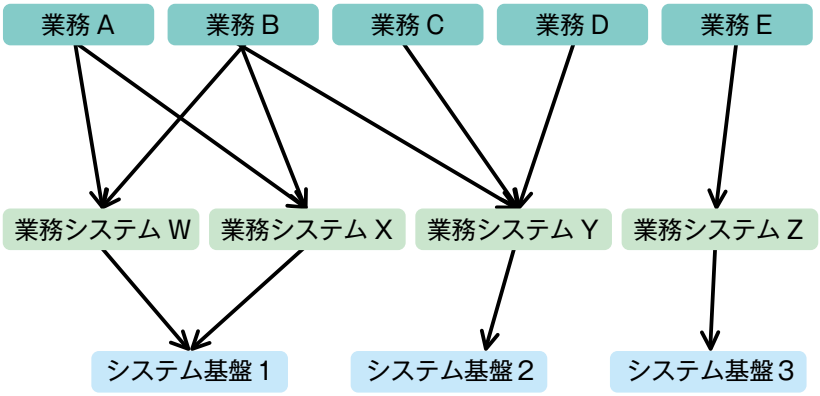
		経営層	事業部門	情報システム部門
導入手順	検討対象の選定	選定	重要業務・優先順位の提示	システム基盤の識別
	モデルシステムの選定	選定	事前準備（目標復旧時間など）	事前準備（投資額など）
	要件定義	承認	確認	要件の調整・確定
	導入計画策定	承認	確認	策定

3.3. 検討対象の選定の概要

検討対象の選定では、高回復力システム基盤の適用範囲を特定するため、以下の２点を明らかにします。

① 重要業務
② その業務を支えるシステム基盤

重要業務を選定すれば、その業務で利用する業務システムが特定され、その業務システムが稼働するシステム基盤を検討対象にすることが出来るからです。業務、業務システム、システム基盤の関係を例示すると図 3.3-1 のようになります。



■図 3.3-1　業務、業務システム、システム基盤の関係例

検討対象の選定は、以下の手順で進めます。なお、手順は、既存のシステム基盤を対象にするケースを想定しています。新規に高回復力システム基盤を導入する場合においては、手順２のモデルシステムの選定から進めてください。

（１）重要業務の識別

重要業務で利用する業務システムが稼働するシステム基盤を選ぶため、最初に重要業務を識別します。重要業務とは、業務が中断することによって、売上や収益が大幅に落ちる、組織の社会的な信用を失墜させる、顧客などとの契約違反が生じ多額の損害賠償や重要な顧客などの喪失が発生する、など事業に大きな影響を及ぼす可能性がある業務です。

（2）システム基盤の識別

重要業務で利用する業務システムが稼働するシステム基盤を識別します。図 3.3-1 に示すように、業務システムとシステム基盤は、一対一とならないことがあります。ここでは重要業務で利用する業務システムが稼働するシステム基盤を全て検討対象とします。

（3）優先順位の決定

検討対象としたシステム基盤が多い場合には、優先順位を決めて、順次導入（対策の強化を含む）していくことになります。この場合、業務の重要度が優先順位の主要な決定理由となりますが、そのシステム基盤を利用する重要業務の数や将来の情報システムのリプレース計画なども考慮する必要があります。

3.4. モデルシステムの選定の概要

モデルシステムの選定作業では、以下の手順で検討対象のシステム基盤に適用する高回復力システム基盤のモデルシステムを選定します。

（1）モデルシステム選定のための事前調査

情報システム部門は、選定した検討対象のシステム基盤で稼働する各業務について、表 3.4-1 で示す各モデルシステムの想定脅威ごとの復旧時間や次頁の（3）に記載しているモデルシステム選定のポイントなどを基に、事業部門と必要な業務の目標復旧時間について協議します。

次にモデルシステムの候補について、経営層の意志決定を仰ぐために必要な情報を準備します。必要な情報には、高回復力システム基盤の導入や維持に必要な投資規模や要員体制などがあります。

なお、投資規模や体制は、複数のモデルシステムのケースについて提供し、経営層が費用対効果を考慮してモデルシステムを選定できるようにする必要があります。

■表 3.4-1　モデルシステムの概要

モデル	想定脅威	業務の目標復旧時間	説明
1	大規模システム障害	1～3日	大規模システム障害時において、復旧までに数日を要しても組織の存続に致命的な影響を与えないと考えられるシステム
	大規模災害	1～6ヶ月	大規模災害時において、復旧までに比較的期間を要しても組織の存続に致命的な影響を与えないと考えられるシステム
2	大規模システム障害	2時間以内	大規模システム障害時において、長時間の停止が発生した場合に業績など会社に大きなダメージを与えるシステム
	大規模災害	1～6ヶ月	大規模災害時において、復旧までに比較的期間を要しても組織の存続に致命的な影響を与えないと考えられるシステム
3	大規模システム障害	2時間以内	大規模システム障害時において、長時間、停止した場合、組織の存続や業績に多大な影響を与えるシステム
	大規模災害	1～7日間	大規模災害時において、長期間、停止した場合、組織の存続や業績に多大な影響を与えるシステム
4	大規模システム障害	2時間以内	大規模システム障害時において、長時間、停止した場合、組織の存続や業績に多大な影響を与えるシステム
	大規模災害	2時間以内	大規模災害時において社会的な要請や組織の戦略上、短時間での復旧が必要となるシステム

（２）モデルシステムの選定

経営層は、モデルシステムが提示する業務の復旧時間などの特徴や情報システム部門が提示する投資規模などを基に検討対象のシステム基盤に適切なモデルシステムを選定します。なお、選定にあたっては、情報システム部門だけでなく、関係する事業部門の長などとも意見交換を行うことが必要です。

（３）各モデルシステム選定のポイント

各モデルシステムの選定のポイントは以下のとおりです。

①モデルシステム１の選定例

大規模なシステム障害時には再開までに最大３日間を要しても事業に致命的な影響を与えないと考えられる業務や、数日であれば手作業で継続できる業務であり、大規模災害発生時のような非常事態の際には、比較的長期間の停止が許される業務が該当します。例えば、経理業務や人事業務などの社内業務の多くは、これに該当すると考えられます。決算業務などについても大規模災害などで被災した企業に対して決算発表が猶予されるなどの措置がとられています。

②モデルシステム２の選定例

大規模なシステム障害時には、２時間以内で再開しなければ、事業に大きな影響を与える業務ですが、モデルシステム１と同様に大規模災害発生時のような非常事態の際には、比較的長期間の停止が許される業務が該当します。例えば、生産、販売、物流などの業務で、業務規模が大きくなく災害時には代替手段で業務継続をできるようにしている場合などが該当します。

③モデルシステム３の選定例

大規模なシステム障害時には、２時間以内で再開しなければ、事業に大きな影響を与える業務で、大規模災害発生時のような非常事態の際にも、１～７日程度で復旧する必要がある業務が該当します。多くの組織の生産、販売、物流などの基幹業務が該当します。

④モデルシステム４の選定例

大規模なシステム障害時においても、また大規模な災害発生時においても、２時間以内での再開が必要な業務の場合が該当します。社会インフラを担う業務や国内全域やグローバルに展開している業務など、短期間でも業務の中断による影響が大きな業務がこれに該当します。

３．５．要件定義の概要

モデルシステムの要件定義では、導入する高回復力システム基盤の要件定義を行います。

モデルシステムを選定すると、各モデルシステムの高回復力システム基盤に必要と考えられる要件が示されます。ただし、各モデルシステムが提示している要件は、各組織の事情や既存のシステム環境などによって、調整が必要となる場合があります。例えば、モデルシステムが要求するメインサイトの耐震性は震度６弱までですが、ベンダの提供する情報処理施設を活用することが前提であれば、要件を震度６強以上に変更するなどが挙げられます。

なお、「計画編」では、要件調整のより詳しい手順や各要件を確認する際の留意点が記述されているので要件定義を行う際に参照してください。

3.6. 導入計画策定の概要

導入計画は、対象となるシステム基盤に対して具体的な対策の導入を行うための計画です。この計画は事業部門と経営層の承認を得て実施される必要があります。導入計画の策定にあたっての主要な作業を下記に示します。

(1) 現状のシステム基盤のギャップ分析と対策手段などの検討

確定した要件について、現状のシステム基盤とのギャップ分析を行い、ギャップを解消するための対策手段を検討します。

対策手段には、主要な機器の冗長化、データなどのバックアップの遠隔地保管、情報処理施設の耐震強化などがあります。

(2) スケジュールおよびコスト見積もり

上記の対策手段の導入にかかる期間や費用を明らかにします。

(3) 導入や運用にかかる要員などの体制の検討

対策手段の導入やその後の運用に必要となる要員などの体制について検討します。また、事業や技術の動向に合わせて対策手段などの見直しを行う必要があるため、評価や見直しの時期や条件なども決めておく必要があります。

おわりに

本ガイド（概要編）では、大規模システム障害や大規模災害の発生時において事業継続のために重要となる、情報システムの回復力を高めるための対策の概要について平易に解説しました。

これまで事業継続計画（BCP）の策定に躊躇されていた組織も少なくないと思われますが、事業活動に必要な回復時間等に応じた４つの高回復力システム基盤の「モデルシステム」により、経営層の方が情報システム部門の支援を得つつより適切な意思決定がしやすくなり、BCP の策定に寄与するものと考えます。

ご理解いただいたことを実践し、大規模災害や大規模障害の際に情報システムを停止させないための対策と、万が一情報システムが停止してしまった場合に迅速に復旧するための事前準備を適切に行い、事業継続性をより高めより確実にしていただきたいと思います。計画編では、その実践の手順について具体的に説明します。

参考情報

・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に経済産業省が策定したガイドライン
「ＩＴサービス継続ガイドライン」
http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf

・高回復力システム基盤の要件を導出する基礎とした非機能要求グレード一式がダウンロードできる Web サイト
非機能要求の見える化と確認の手段を実現する「非機能要求グレード」の公開～システム基盤における非機能要求の見える化ツール～， 2010 年４月，
独立行政法人情報処理推進機構 技術本部ソフトウェア・エンジニアリング・センター
http://sec.ipa.go.jp/reports/20100416.html

編著者

ＩＴサービス継続ＷＧ

ＩＴサービス継続ＷＧ（50音順　氏名／所属／敬称略）

主査　榎木　千昭　　慶應義塾大学　商学研究科
委員　市川　順之　　伊藤忠テクノソリューションズ株式会社
委員　伊藤　毅　　株式会社富士通総研
委員　江刺　勲　　日本電気株式会社
委員　勝俣　良介　　ニュートン・コンサルティング株式会社
委員　加藤　雅彦　　株式会社インターネットイニシアティブ
委員　駒瀬　彰彦　　株式会社アズジェント
委員　齋藤　和則　　シースリー・マネージメント株式会社
委員　佐藤　直之　　日本ベリサイン株式会社
委員　芝　　勝徳　　神戸市外国語大
委員　原田　要之助　情報セキュリティ大学院大学

技術本部ソフトウエア・エンジニアリング・センター事務局

山下　博之
柏木　雅之
在田　博明
河村　太郎
高橋　圭二
三好　進

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan