高回復力システム基盤導入ガイド

計画編

2012 年 5 月

独立行政法人情報処理推進機構(IPA)
技術本部ソフトウェア・エンジニアリング・センター(SEC)

目次

1. 導入ガイドの目的と構成

1.1. 導入ガイドの目的

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ある。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ある。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る。

高回復力システム基盤導入には、多大な労力を要するとともに、豊富な経験が必要になる。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」という。）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る。

1.2. 導入ガイドの構成

導入ガイドは、以下の文書から構成される。

表 1.2-1 高回復力システム基盤導入ガイドの構成

No	文書名	公開日	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

(1)概要編は、高回復力システム基盤の必要性、企画・要件定義プロセスの概要、導入ガイドの特徴であるモデルシステムの概要について説明している。
特にモデルシステム選定段階で重要な意思決定者となる経営層および事業部門が理解、利用できる内容となるよう留意している。

(2)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構築導入する際の、企画・要件定義プロセスに、およびモデルシステムの詳細について説明している。
特に情報システム部門を主とする「導入プロジェクト」の実務担当者向けに、検討対象の選定、モデルの選定、要件定義、導入計画策定の各作業手順展開、留意点などについて、実用的な情報を提供できるようにした。

(3)事例編は、高回復力システム基盤の具体的な構築導入事例や構築導入の際のポイントなどを解説している。

2. 計画編の基本的な考え方

2.1. 高回復力要件

情報システムに関する要求は、業務実現に直接関係する「機能要求」と、性能、信頼性、拡張性、セキュリティなど、機能要求以外のもの全般を指す「非機能要求」に大別される。
非機能要求は主にシステム基盤、すなわちハードウェア・設備、OS やミドルウェア、運用管理の仕組みや体制などに反映されるものであり、導入ガイドにおける「要件定義」とは、「高回復力システム基盤」の非機能要求を明確化することに他ならない。
計画編では、モデルシステムを利用して要件定義を行うために必要な、大規模システム障害および大規模災害からの「高回復力」に影響する非機能要求項目(要件)として、「可用性」、「運用・保守性」、「システム環境」に関する 37 件を選定した。以降計画編では「高回復力要件」と呼ぶ。
高回復力要件には以下の 3 種類がある。

(1)前提要件 (5 件)

前提要件とは、高回復力システム基盤を導入するにあたって前提となる要件である。高回復力要件の定義において、最初に決めておく必要がある。モデルシステム毎の特徴、業務の目標回復時間などを目安に、各要件の内容を設定する。表 2.2-1 に前提要件の一覧を示す。

(2)主要要件 (27 件)

主要要件とは、前提要件を実現するために必要となる、施設や機器などの構成、バックアップ方式などに係る要件である。モデルシステム毎にあらかじめ要件内容が設定されており、必要に応じて要件内容の調整を行う。表 2.2-2 に主要要件の一覧を示す。

(3)考慮要件 (5 件)

考慮要件とは、前提条件および主要要件以外に高回復力システム基盤の構築にあたって、考慮しなければならない要件である。モデルシステムに依存せず、組織の要員体制やベンダとの役割分担などの状況によって決める必要がある。表 2.2-3 に考慮要件の一覧を示す。

表 2.2-1 前提要件一覧

非機能要求				
項番	大項目	中項目	小項目	要件
A.1.2.3	可用性	継続性	業務継続性	業務継続の要求度
A.1.3.1			目標復旧水準 (業務停止時)	RPO(目標復旧地点)
A.1.3.2				RTO(目標復旧時間)
A.1.3.3				RLO(目標復旧レベル)
A.1.4.1			目標復旧水準	システム再開目標

表 2.2-2 主要要件一覧

非機能要求				
項番	大項目	中項目	小項目	要件
A.2.1.1	可用性	耐障害性	サーバ	冗長化(機器)
A.2.1.2				冗長化(コンポーネント)
A.2.3.1			ネットワーク機器	冗長化(機器)

非機能要求				
項番	大項目	中項目	小項目	要件
A.2.3.2				冗長化（コンポーネント）
A.2.4.1			ネットワーク	回線の冗長化
A.2.4.2				経路の冗長化
A.2.5.1			ストレージ	冗長化（機器）
A.2.5.2				冗長化（コンポーネント）
A.2.5.3				冗長化（ディスク）
A.2.6.1			データ	バックアップ方式
A.2.6.3				データインテグリティ
A.3.1.1		災害対策	システム	復旧方針
A.3.2.1			外部保管データ	保管場所分散度
A.3.2.2				保管方法
C.1.3.1	運用・保守性	通常運用	運用監視	監視情報
C.1.3.2				監視間隔
C.2.5.1		保守運用	定期保守頻度	定期保守頻度
C.2.6.1			予防保守レベル	予防保守レベル
C.3.2.1		障害時運用	障害復旧自動化の範囲	障害復旧自動化の範囲
C.3.3.1			システム異常検知時の対応	対応可能時間
C.3.3.2				駆けつけ到着時間
C.3.3.3				SE 到着平均時間
C.3.4.1			交換用部材の確保	保守部品確保レベル
C.3.4.2				予備機の有無
C.4.3.1		運用環境	マニュアル準備レベル	マニュアル準備レベル
F.4.1.1	システム環境	機材設置環境条件	耐震/免震	耐震震度
F.4.4.4			電気設備適合性	停電対策

表 2.2-3 考慮要件一覧

非機能要求				
項番	大項目	中項目	小項目	要件
C.5.5.1	運用・保守性	サポート体制	一次対応役割分担	一次対応役割分担
C.5.6.3			サポート要員	ベンダ側対応者の要求スキルレベル
C.5.8.2			オペレーション訓練	オペレーション訓練範囲
C.5.9.1			定期報告会	定期報告会実施頻度
C.5.9.2				報告内容のレベル

「大項目」は非機能要求を目的、対象範囲の単位でまとめた分類、

「中項目」は非機能要求を検討課題、主題の単位でまとめた分類、

「小項目」は非機能要求の内容を論理的に記述し得る単位、

「要件(非機能要求項目)」は非機能要求の内容を定量的に表現し得る最小単位である。

2.2. モデルシステムと要件調整

各非機能要求項目の要件内容を定義することは容易ではない。それが何十もの数となるとなおさらである。
そこで計画編では、高回復力要件 37 件に対して、設定可能な要求内容の候補を準備している。
すなわち、各要件について、複数の要求レベル(実現すべき回復力の度合い)に対応した要件内容をあらかじめ設定し、選択肢として提示されるようにしている。
さらに、主要要件 27 件については、モデルシステムを選択することにより、標準(デフォルト)の要件内容のセットが提示されるようにしている。
導入ガイドの利用者は、選定したモデルシステムに設定されている標準の要件内容の妥当性を吟味し、必要に応じて変更することができる。これにより、対象システム基盤の制約条件などに即して、きめ細かく要件を定義することができる。計画編では、これを「要件調整」と称している。

2.3. 計画編における非機能要求グレードの利用

高回復力要件の枠組みは、非機能要求グレード(2010/04, IPA/SEC)中の「非機能要求項目一覧」に準じている。
非機能要求グレードは、非機能要求項目を体系的に整理し、項目毎にレベル付けした選択肢を提示し、情報システム構築の受発注者間での要件定義内容に関する合意を明確化するためのツールである。
計画編における「要件」は、非機能要求項目一覧における最小単位である「メトリクス(指標)」に相当する。
計画編は、非機能要求グレードに関する知識がなくても理解できるよう説明を加えており、利用に際して非機能要求グレードを参照する必要はない。
なお、非機能要求項目一覧との対応が可能となるよう、要件の識別番号「項番」に非機能要求項目の「項番」をそのまま使用しているため、番号の値に「飛び」が見られる。

3. モデルシステム

3.1. モデルシステムの特徴

「導入ガイド」では、検討対象(システム基盤)の要件定義を迅速化するためのツールとして、モデルシステムを提供している。
4 つのモデルシステムは、主に①耐障害性・耐災害性、②目標復旧時間(RTO)、③投資規模の大小 の観点でそれぞれ特徴を備え、その特徴を実現するための要件の組合せを持つ。

本章ではモデルシステム毎の特徴を表形式で示す。

3.1.0. 共通要件

「高回復力」を備えることの前提として、すべてのモデルシステムは以下の要件を満たしているものとする。

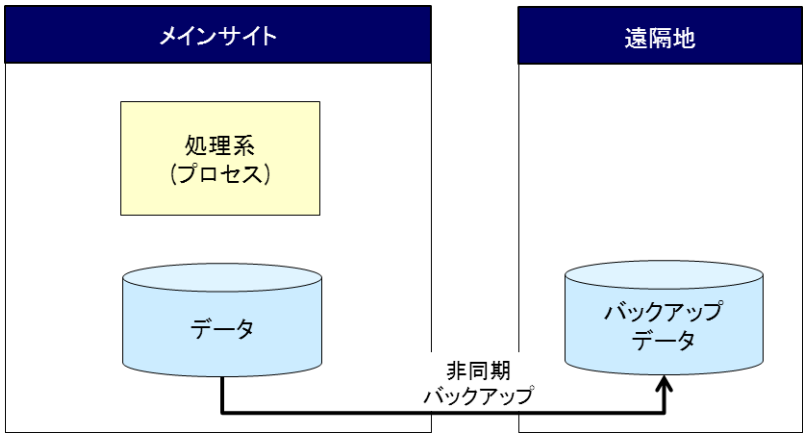
表 3.1.0-1 モデルシステム共通要件

全モデルシステムに共通する要件
・建物・設備は震度 6 弱の地震に耐える。 ・サーバやストレージの重要なコンポーネント(CPU モジュール、ディスクコントローラなど)は冗長化されている。 ・ディスクは RAID(0 以外)構成されている。 ・通信回線のうち、重要な経路は冗長化されている。

3.1.1. モデルシステム 1

高回復力システム基盤の最小構成。

モデル 1 のイメージ



特徴	① 必要となるシステム基盤の強度 (災害や障害への耐性)	低 (4 モデル間の相対値)
	② 業務再開までの 目標復旧時間(RTO)	大規模システム障害　1～3 日 大規模災害　1～6 ヶ月
	③ システム基盤導入のための投資規模	低 (4 モデル間の相対値)

構成	① バックアップデータの取得方式、 取得間隔	非同期 月次
	② 機器の冗長化	なし メインサイトのシステム(処理系)はシングル 回線(物理的伝送路)および経路は一部冗長化
	③ バックアップサイト	なし バックアップシステムは持たない バックアップデータを遠隔地に保管

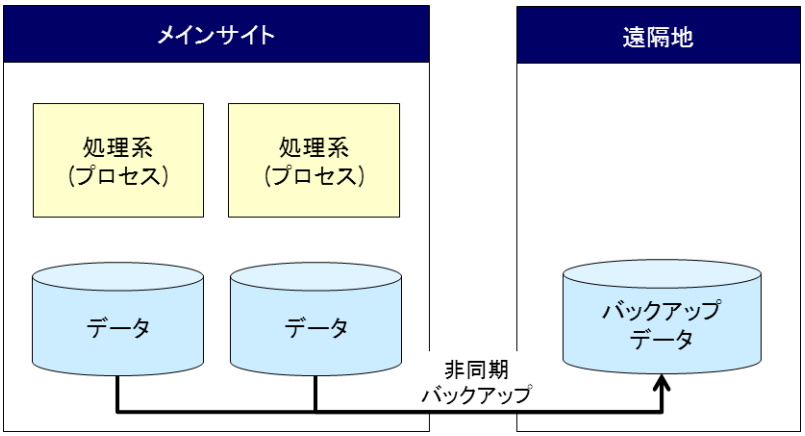
非機能要求					モデル 1 の要件
項番	大項目	中項目	小項目	要件	
A.2.1.1	可用性	耐障害性	サーバ	冗長化(機器)	非冗長構成
A.2.1.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.3.1			ネットワーク機器	冗長化(機器)	特定の機器のみ冗長化
A.2.3.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.4.1			ネットワーク	回線の冗長化	一部冗長化
A.2.4.2				経路の冗長化	一部冗長化
A.2.5.1			ストレージ	冗長化(機器)	非冗長構成
A.2.5.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.5.3				冗長化(ディスク)	RAID5 による冗長化
A.2.6.1			データ	バックアップ方式	オフラインバックアップ

非機能要求					モデル 1 の要件
項番	大項目	中項目	小項目	要件	
A.2.6.3				データインテグリティ	データの完全性を保障（エラー検出と訂正）
A.3.1.1		災害対策	システム	復旧方針	限定された構成をバックアップサイトで構築
A.3.2.1			外部保管データ	保管場所分散度	1ヵ所(遠隔地)
A.3.2.2				保管方法	媒体による保管
C.1.3.1	運用・保守性	通常運用	運用監視	監視情報	死活監視
C.1.3.2				監視間隔	リアルタイム監視（分間隔）
C.2.5.1		保守運用	定期保守頻度	定期保守頻度	年 1 回
C.2.6.1			予防保守レベル	予防保守レベル	定期保守時に検出した予兆の範囲で対応
C.3.2.1		障害時運用	障害復旧自動化の範囲	障害復旧自動化の範囲	一部の障害復旧作業を自動化
C.3.3.1			システム異常検知時の対応	対応可能時間	ベンダの営業時間内（例：9 時～17 時）で対応
C.3.3.2				駆けつけ到着時間	保守員到着が異常検知からユーザの翌営業開始時まで対応
C.3.3.3				SE 到着平均時間	SE 到着が異常検知からユーザの翌営業開始時まで対応
C.3.4.1			交換用部材の確保	保守部品確保レベル	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する
C.3.4.2				予備機の有無	予備機なし
C.4.3.1		運用環境	マニュアル準備レベル	マニュアル準備レベル	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供
F.4.1.1	システム環境	機材設置環境条件	耐震/免震	耐震震度	震度 6 弱相当（250 ガル）
F.4.4.4			電気設備適合性	停電対策	10 分

3.1.2. モデルシステム 2

モデル 1 のシステムを 2 重化し、耐障害性を向上させたパターン。

モデル 2 のイメージ



特徴	① 必要となるシステム基盤の強度 (災害や障害への耐性)	中 (4 モデル間の相対値)
	② 業務再開までの 目標復旧時間(RTO)	大規模システム障害　2 時間以内 大規模災害　1～6 ヶ月
	③ システム基盤導入のための投資規模	中 (4 モデル間の相対値)

構成	① バックアップデータの取得方式、 取得間隔	非同期 週次
	② 機器の冗長化	あり メインサイトのシステム(処理系)を 2 重化 回線(物理的伝送路)および経路は一部冗長化
	③ バックアップサイト	なし バックアップシステムは持たない バックアップデータのみ遠隔地に保管

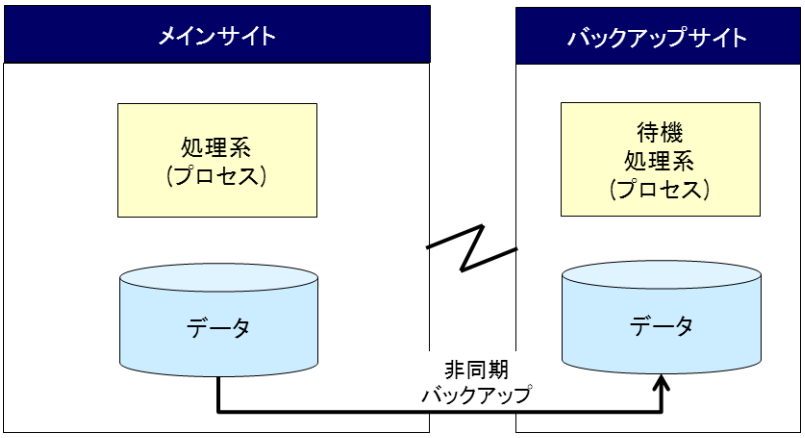
非機能要求					モデル 2 の要件
項番	大項目	中項目	小項目	要件	
A.2.1.1	可用性	耐障害性	サーバ	冗長化(機器)	全てのサーバで冗長化
A.2.1.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.3.1			ネットワーク機器	冗長化(機器)	全ての機器を冗長化
A.2.3.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.4.1			ネットワーク	回線の冗長化	一部冗長化
A.2.4.2				経路の冗長化	一部冗長化
A.2.5.1			ストレージ	冗長化(機器)	全ての機器を冗長化
A.2.5.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.5.3				冗長化(ディスク)	RAID5 による冗長化
A.2.6.1			データ	バックアップ方式	オフラインバックアップ

非機能要求					モデル 2 の要件
項番	大項目	中項目	小項目	要件	
A.2.6.3				データインテグリティ	データの完全性を保障（エラー検出と訂正）
A.3.1.1		災害対策	システム	復旧方針	限定された構成をバックアップサイトで構築
A.3.2.1			外部保管データ	保管場所分散度	1ヵ所(遠隔地)
A.3.2.2				保管方法	媒体による保管
C.1.3.1	運用・保守性	保守運用	運用監視	監視情報	死活監視
C.1.3.2				監視間隔	リアルタイム監視（分間隔） または リアルタイム監視（秒間隔）
C.2.5.1			定期保守頻度	定期保守頻度	年 1 回
C.2.6.1			予防保守レベル	予防保守レベル	定期保守時に検出した予兆の範囲で対応
C.3.2.1		運用環境	障害復旧自動化の範囲	障害復旧自動化の範囲	一部の障害復旧作業を自動化
C.3.3.1			システム異常検知時の対応	対応可能時間	ユーザの指定する時間帯（例：18 時～24 時）で対応
C.3.3.2				駆けつけ到着時間	保守員到着が異常検知から数時間内
C.3.3.3				SE 到着平均時間	SE 到着が異常検知から数時間内
C.3.4.1			交換用部材の確保	保守部品確保レベル	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保
C.3.4.2				予備機の有無	予備機なし
C.4.3.1			マニュアル準備レベル	マニュアル準備レベル	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供
F.4.1.1	システム環境	機材設置環境条件	耐震/免震	耐震震度	震度 6 弱相当（250 ガル）
F.4.4.4			電気設備適合性	停電対策	1 時間

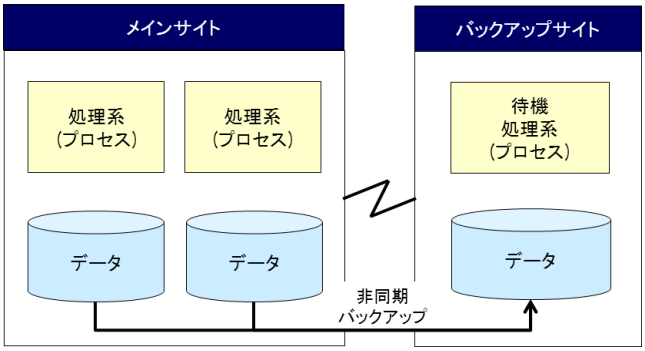
3.1.3. モデルシステム 3

バックアップサイトを備えるパターン。

モデル 3 のイメージ



メインサイトを 2 重化(オプション)



特徴	① 必要となるシステム基盤の強度 (災害や障害への耐性)	高 (4 モデル間の相対値)
	② 業務再開までの 目標復旧時間(RTO)	大規模システム障害　2 時間以内 大規模災害　1～7 日間
	③ システム基盤導入のための投資規模	高 (4 モデル間の相対値)

構成	① バックアップデータの取得方式、 取得間隔	非同期 数回/日
	② 機器の冗長化	あり メインサイトのシステム(処理系)を必要に応じて 2 重化
	③ バックアップサイト	あり 待機システム

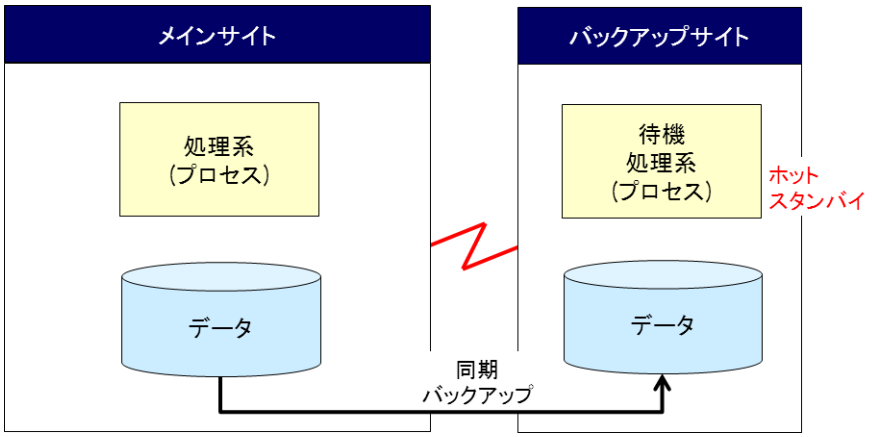
非機能要求					モデル 3 の要件
項番	大項目	中項目	小項目	要件	
A.2.1.1	可用性	耐障害性	サーバ	冗長化(機器)	全てのサーバで冗長化
A.2.1.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.3.1			ネットワーク	冗長化(機器)	全ての機器を冗長化

非機能要求					モデル 3 の要件
項番	大項目	中項目	小項目	要件	
A.2.3.2			機器	冗長化（コンポーネント）	特定のコンポーネントのみ冗長化
A.2.4.1			ネットワーク	回線の冗長化	一部冗長化
A.2.4.2				経路の冗長化	一部冗長化
A.2.5.1			ストレージ	冗長化（機器）	全ての機器を冗長化
A.2.5.2				冗長化（コンポーネント）	特定のコンポーネントのみ冗長化
A.2.5.3				冗長化（ディスク）	RAID5 による冗長化
A.2.6.1			データ	バックアップ方式	オフラインバックアップ
A.2.6.3				データインテグリティ	データの完全性を保障（エラー検出と訂正）
A.3.1.1		災害対策	システム	復旧方針	限定された構成をバックアップサイトで構築
A.3.2.1			外部保管データ	保管場所分散度	1 ヵ所(遠隔地)
A.3.2.2				保管方法	バックアップサイトへのリモートバックアップ
C.1.3.1	運用・保守性	通常運用	運用監視	監視情報	死活監視
C.1.3.2			運用監視	監視間隔	リアルタイム監視（分間隔） または リアルタイム監視（秒間隔）
C.2.5.1		保守運用 保守運用	定期保守頻度	定期保守頻度	年 1 回
C.2.6.1			予防保守レベル	予防保守レベル	定期保守時に検出した予兆の範囲で対応
C.3.2.1		障害時運用	障害復旧自動化の範囲	障害復旧自動化の範囲	一部の障害復旧作業を自動化
C.3.3.1			システム異常検知時の対応	対応可能時間	24 時間対応
C.3.3.2				駆けつけ到着時間	保守員到着が異常検知から数時間内
C.3.3.3				SE 到着平均時間	SE 到着が異常検知から数時間内
C.3.4.1			交換用部材の確保	保守部品確保レベル	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保
C.3.4.2				予備機の有無	予備機なし
C.4.3.1		運用環境	マニュアル準備レベル	マニュアル準備レベル	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供
F.4.1.1	システム環境	機材設置環境条件	耐震/免震	耐震震度	震度 6 弱相当（250 ガル）
F.4.4.4			電気設備適合性	停電対策	1 時間

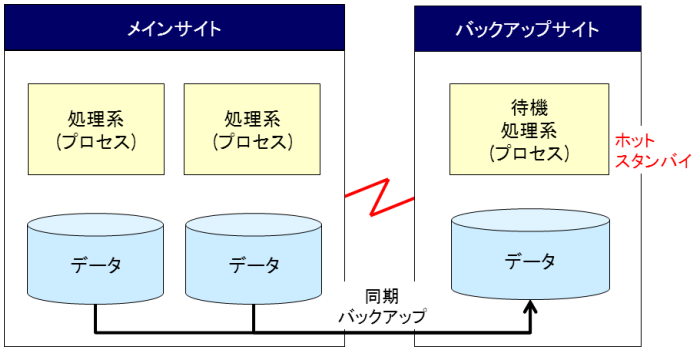
3.1.4. モデルシステム 4

データバックアップの頻度を高め、大規模災害時の RTO を短縮したパターン。

モデル 4 のイメージ



メインサイトを 2 重化(オプション)



特徴	① 必要となるシステム基盤の強度 (災害や障害への耐性)	高 (4 モデル間の相対値)
	② 業務再開までの 目標復旧時間(RTO)	大規模システム障害　2 時間以内 大規模災害　2 時間以内
	③ システム基盤導入のための投資規模	高 (4 モデル間の相対値)

構成	① バックアップデータの取得方式、取得間隔	同期 数回/時
	② 機器の冗長化	あり メインサイトのシステム(処理系)を必要に応じて 2 重化
	③ バックアップサイト	あり ホットスタンバイ

非機能要求					モデル 4 の要件
項番	大項目	中項目	小項目	要件	
A.2.1.1	可用性	耐障害性	サーバ	冗長化(機器)	全てのサーバで冗長化
A.2.1.2				冗長化(コンポーネント)	特定のコンポーネントのみ冗長化
A.2.3.1			ネットワーク	冗長化(機器)	全ての機器を冗長化

非機能要求					モデル 4 の要件
項番	大項目	中項目	小項目	要件	
A.2.3.2			機器	冗長化（コンポーネント）	特定のコンポーネントのみ冗長化
A.2.4.1			ネットワーク	回線の冗長化	全て冗長化
A.2.4.2				経路の冗長化	全て冗長化
A.2.5.1			ストレージ	冗長化（機器）	全ての機器を冗長化
A.2.5.2				冗長化（コンポーネント）	特定のコンポーネントのみ冗長化
A.2.5.3				冗長化（ディスク）	RAID5 による冗長化
A.2.6.1			データ	バックアップ方式	オンラインバックアップ または オフラインバックアップとオンラインバックアップの組合せ
A.2.6.3				データインテグリティ	データの完全性を保障（エラー検出と訂正）
A.3.1.1		災害対策	システム	復旧方針	限定された構成をバックアップサイトで構築
A.3.2.1			外部保管データ	保管場所分散度	1 ヵ所(遠隔地)
A.3.2.2				保管方法	バックアップサイトへのリモートバックアップ
C.1.3.1	運用・保守性	通常運用	運用監視	監視情報	パフォーマンス監視
C.1.3.2				監視間隔	リアルタイム監視（秒間隔）
C.2.5.1		保守運用	定期保守頻度	定期保守頻度	年 1 回
C.2.6.1			予防保守レベル	予防保守レベル	定期保守時に検出した予兆の範囲で対応
C.3.2.1		障害時運用	障害復旧自動化の範囲	障害復旧自動化の範囲	一部の障害復旧作業を自動化
C.3.3.1			システム異常検知時の対応	対応可能時間	24 時間対応を行う
C.3.3.2				駆けつけ到着時間	保守員が常駐
C.3.3.3				SE 到着平均時間	SE が常駐
C.3.4.1			交換用部材の確保	保守部品確保レベル	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保
C.3.4.2				予備機の有無	予備機なし
C.4.3.1		運用環境	マニュアル準備レベル	マニュアル準備レベル	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供
F.4.1.1	システム環境	機材設置環境条件	耐震/免震	耐震震度	震度 6 弱相当（250 ガル）
F.4.4.4			電気設備適合性	停電対策	1 時間

3.2. モデルシステムのバリエーション

モデルシステム選定に際して投資規模を概算する、導入計画策定のためにシステム基盤の機器構成、採用技術、運用体制などに関するイメージを具体化する、といった場合に、モデルシステムに対して、実装をイメージしたバリエーションを想定してみることが有用である。

図 3.2-1、図 3.2-2、図 3.2-3 にバリエーションの例を示す。

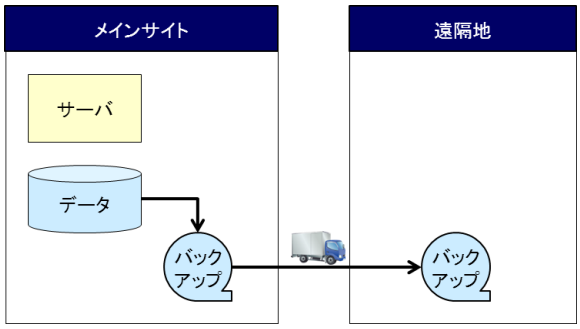


図 3.2-1 モデル 1 およびモデル 2(メインサイトのサーバなどは冗長化)で、バックアップデータを MT に格納し、遠隔地に保管する例

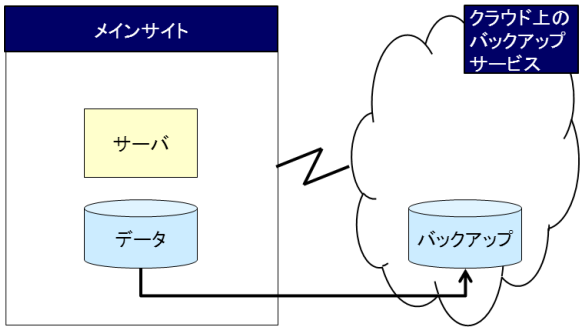


図 3.2-2 モデル 1 およびモデル 2(メインサイトのサーバなどは冗長化)で、クラウドのデータバックアップサービスを利用する例

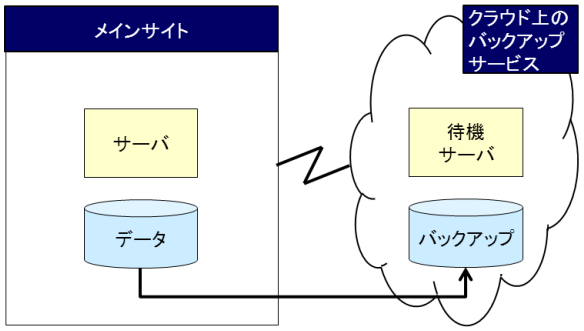


図 3.2-3 モデル 3 およびモデル 4 で、クラウドのシステムバックアップサービスを利用する例

4. 高回復力システム基盤導入計画

ここでは、高回復力システム基盤を導入するため、どのように計画し、進めていくか、また、モデルシステムをどのように活用するかを解説する。
なお、作業手順を記述するに当たり、共通フレーム 2007 (第 2 版)(2009/10, IPA/SEC)の概念、用語を準用する。

表 4-1 共通フレーム 2007 の作業分解構造

作業	定義
プロセス	システム開発作業を役割の観点でまとめたもの
アクティビティ	プロセスの構成要素
タスク	アクティビティの構成要素
リスト	タスクの構成要素

計画編で取扱う領域全体を共通フレームの「企画プロセス」「要件定義プロセス」レベルに相当する「プロセス」とみなし、その構成要素は分解階層にしたがい、「アクティビティ」、「タスク」、「リスト」とする。
ただしアクティビティ、タスク、リストの作業名は、導入ガイド固有のものであり、共通フレームとは一致しない。

計画編では、以下に示す 4 アクティビティで、導入計画策定に至る。

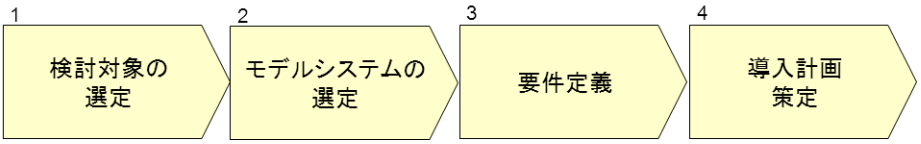


図 4-1 高回復力システム基盤導入計画の手順

(1)アクティビティ 1 検討対象の選定
重要業務に関わるシステム基盤を識別し、重要性、事業戦略、システム投資計画などを勘案して取組みの優先順位を決定する。
(2)アクティビティ 2 モデルシステムの選定
検討対象が目標とする高回復力システム基盤のイメージに合致するモデルシステムを選定する。
(3)アクティビティ 3 要件定義
モデルシステムが持つ要件の「幅」を、検討対象の目標に沿うよう収斂させ、要件を確定する。
(4)アクティビティ 4 導入計画の策定
検討対象の「高回復力システム基盤導入(プロジェクト)」計画を策定する。

4.1. アクティビティ１　検討対象の選定

重要業務に関わるシステム基盤を洗出し、「検討対象」とする。検討対象間の取組みの優先順位を定める。
本工程は、「導入編」においては、主に経営層および事業部門が担当すべき事項とされているが、重要業務に関わるシステム基盤の範囲を適切に識別するためには、情報システム部門の支援が必要である。

本節では、検討対象(システム基盤)選定の根拠が、経営層および事業部門から見て妥当なものとなるよう、重要業務の識別を契機とするアプローチを採用している。
担当者は、組織の特性や制約に応じて、適当な観点/アプローチを検討・採用することが望ましい。

アクティビティ 1 検討対象選定は、以下のタスクで構成される。

(1)タスク 1.1　重要業務の識別
(2)タスク 1.2　システム基盤の識別
(3)タスク 1.3　優先順位決定

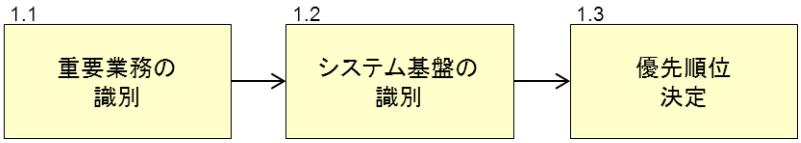


図 4.1-1　検討対象選定の手順

4.1.1. タスク 1.1　重要業務の識別

重要業務を識別、列挙する。

(1)重要業務の定義を確認する。

自社(組織)における重要業務とは何か、確認する。自社内に暗黙知として、あるいは明文化されて共有されている定義が存在しない場合、少なくとも「高回復力システム基盤導入」の関係者間で合意形成しておく必要がある。

重要業務とは、例えば販売・購買・製造・財務などの「業務機能」ではなく、商品・サービス・地域などに関する「セグメント」を切口として識別されるような「事業」の単位と考えると良い。

(2)重要業務の指標を確認する。

業務の「重要性」を判断する基準として、当該セグメントが自社の売上、利益などに占める割合のような、数値化された、「優劣」が明白な指標が採用できれば、重要業務の識別はある程度機械的に実施可能である。非営利組織などにおいては、公共性や社会的使命といった観点から、事業間の「優劣」を定めることになり、指標設定自体が容易ではなかろうと想像する。営利企業においても、社会基盤(インフラストラクチャ)への関与度合いや CSR 方針などを考慮に入れる場合には同様である。

各指標における「重要」「重要でない」の境界値を再確認する。存在しない場合には(1)と同様の対処が必要である。

(3)重要業務を識別する。

(2)の指標を用いて、重要業務を識別、列挙する。

4.1.2. タスク 1.2　システム基盤の識別

重要業務、業務アプリケーション、システム基盤の関連を辿り、重要業務に関わるシステム基盤を識別、列挙する。

(1)重要業務と業務アプリケーションの対応関係を確認する。

前節で識別された重要業務について、各業務の遂行・実現を支える主要な業務アプリケーションを列挙する。

重要業務と業務アプリケーションの対応表	
重要業務_ID	業務アプリ(論理)_ID
B01	AL01
B01	AL02
B01	AL03
B02	

図 4.1.2-1「重要業務と業務アプリケーションの対応表」のイメージ

(2)業務アプリケーションとシステム基盤の対応関係を確認する。

対象となるのは、アプリケーション、OS、ミドルウェアについては論理および実装レベル、ハードウェアについては実装レベルの実体である。

ハードウェア、OS、ミドルウェアの実装レベルの集合を「システム基盤」の単位とする。

業務アプリケーション(実装)		
業務アプリ(論理)_ID	業務アプリ(実装)_ID	システム基盤_ID
AL01	AL01P01	I01
AL01	AL01P02	I02
AL02	AL02P01	I01
AL03	AL03P01	I01

図 4.1.2-2「業務アプリケーション(実装)」のイメージ

(3)複数のシステム基盤で共有する要素の識別

構造物、電源設備など、複数のシステム基盤で共有する要素については、複数のシステム基盤に重複して含まれるものとして取扱う。

(4)重要業務とシステム基盤の対応関係を識別する。

(1)で得た「重要業務と業務アプリケーションの対応表」と、(2)で得た「業務アプリケーション(実装)」から、重要業務とシステム基盤の対応表が導出できる。

重要業務とシステム基盤の対応表	
重要業務_ID	システム基盤_ID
B01	I01
B01	I02
B02	I01
B03	

図 4.1.2-3「重要業務とシステム基盤の対応表」のイメージ

「重要業務とシステム基盤の対応表」の導出に必要な情報の関連を下図に示す。
表記法は一般的なデータモデルの実体と関連の表現に準ずる。
ただし矢印つき曲線のうち実線は結合・導出の流れを、破線は間接的な結合・導出関係を表している。

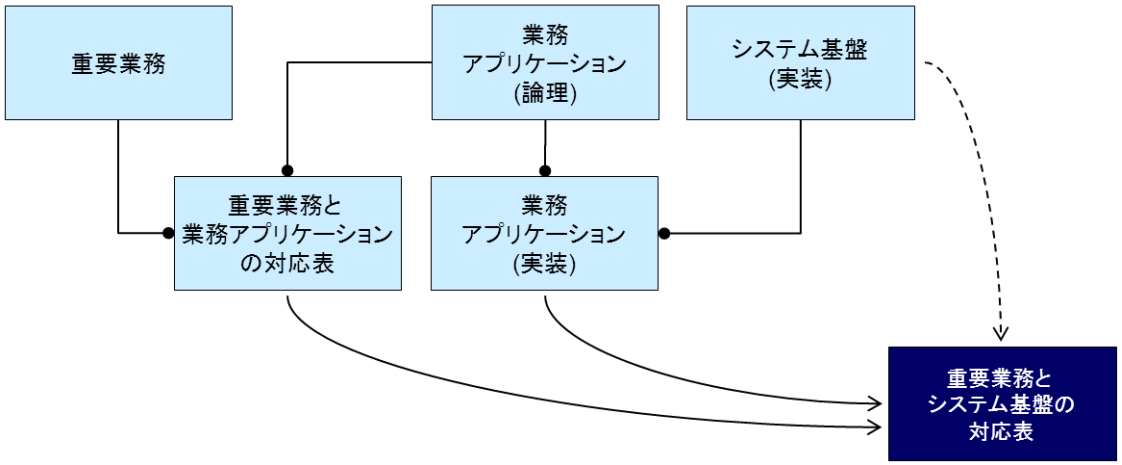


図 4.1.2-4「重要業務とシステム基盤の対応表」導出に必要な情報の関連

4.1.3. タスク 1.3　優先順位決定

必然的に、業務の重要性を主要な因子として、システム基盤の優先順位を定めるのが妥当であろう。さらに既定のシステム投資計画や関連法規の要請などを考慮すれば、より現実的な順位設定を得ることが期待できる。

表 4.1.3-1 優先順位決定のために考慮すべき事項の例

因子	考慮すべき事項
業務の重要性	より重要な業務に関わるシステム基盤から優先して検討対象とする。
当該システム基盤に依存する重要業務の件数	複数の重要業務間の「重要性」の差を無視すれば、より多くの重要業務に関わるシステム基盤の方が、対象として「投資対効果」が高いとみなして良い。
当該システム基盤に関わる中・長期計画	中・長期計画において特定システム基盤の新規導入、更新、廃棄などが決定済みである場合、その時期を考慮する。

4.2. アクティビティ 2 モデルシステムの選定

各検討対象が目標とする回復力のイメージに最も近いモデルシステムを、要件定義のベースとして選定する。本アクティビティは「概要編」においては、主に経営層および事業部門が担当すべき事項とされているが、モデル選定のための前提として、検討対象(業務)の障害時・災害時における要求に適合するか否か、投資規模の概算はどの位か、などの知識を得るためには、情報システム部門の支援が必要である。

アクティビティ 2 モデルシステム選定は、以下のタスクで構成される。

(1)タスク 2.1　モデルシステム「候補」の決定

(2)タスク 2.2　事前評価

(3)タスク 2.3　モデルシステム決定

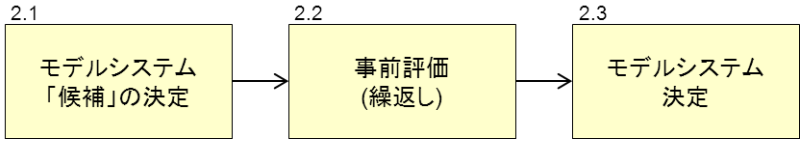


図 4.2-1 モデルシステム選定の手順

4.2.1. タスク 2.1 モデルシステム「候補」の決定

タスク 1.2 で導出した「重要業務とシステム基盤の対応表」、表 4.2.1-1 で説明しているモデルシステムに適したシステムのイメージ、業務の目標復旧時間に合うか否か、などに基づき、検討対象のベースとするのに適当なモデルシステム「候補」を 1～2 件決定する。全モデルの投資規模概算を把握したいのであれば、4 モデルすべてを候補にしても良い。必要であれば、この段階から情報システム部門に支援を求めると良い。

表 4.2.1-1 各モデルシステムに適したシステムのイメージ
(概要編 「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

4.2.2. タスク 2.2　事前評価

事前評価の手順は以下の通り。

(準備)

経営層および事業部門は、情報システム部門に対し、モデルシステム「候補」のシステム構成などに基づき、候補の投資規模(金額、所要期間など)を概算するよう依頼する。

(1)リスト 2.2.1　システム基盤に対する要求などを確認

情報システム部門はモデルシステムの内容を確認し、必要に応じて経営層および事業部門などから情報(システム基盤に対する要求など)を収集し、モデルシステム候補のイメージを、投資規模概算が可能と思われる程度にまで充実させる。

(2)リスト 2.2.2　投資規模概算

各モデルシステム候補の投資規模概算値を算出する。

(3)リスト 2.2.3 「候補」の投資規模概算など確認

情報システム部門は投資規模概算結果を経営層および事業部門に報告・説明する。

報告・説明内容がモデルシステム決定の意思決定のためには不充分であると判断され、経営層および事業部門が再評価、あるいは追加評価を依頼する場合もあり得る。

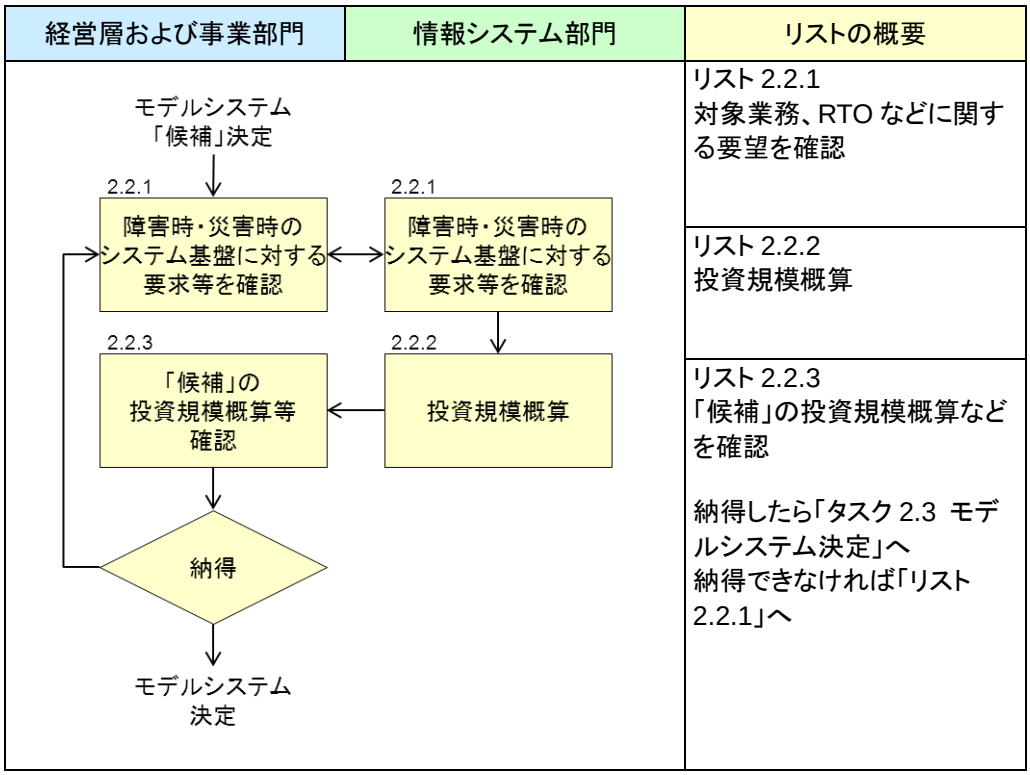


図 4.2.2-1 事前評価の手順

4.2.3. タスク 2.3　モデルシステム決定

事前調査結果などを利用して、検討対象の要件定義ベースとして適当なモデルシステムを決定する。
選定されたモデルシステムの要件は、続く アクティビティ 3　要件定義　において必要に応じて「調整」され、検討対象の要件として確定されるものであり、いわば「叩き台」と考えて良い。

4.3. アクティビティ 3　要件定義

ベースに選定されたモデルシステムを利用して、検討対象の要件を定義する。

アクティビティ 3 要件定義は以下のタスクで構成される。

(1)タスク 3.1　要件定義ワークシート生成

(2)タスク 3.2　要件調整

前提要件 5 件の内容を設定、主要要件 27 件の内容を調整、考慮要件 5 件の設定を定義する。

(3)タスク 3.3　要件確定

要件調整の結果を確認し、高回復力要件を確定する。

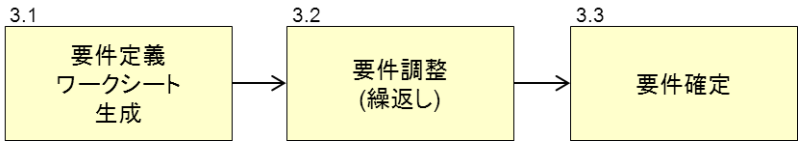


図 4.3-1 要件定義の手順

4.3.1. タスク 3.1　要件定義ワークシート生成

計画編の別添資料として、アクティビティ 3 要件定義の作業を支援するために、要件定義ワークシート(MS EXCEL ファイル)を提供する。

ワークシートの書式は下図の通り(一部折りたたみ可)。

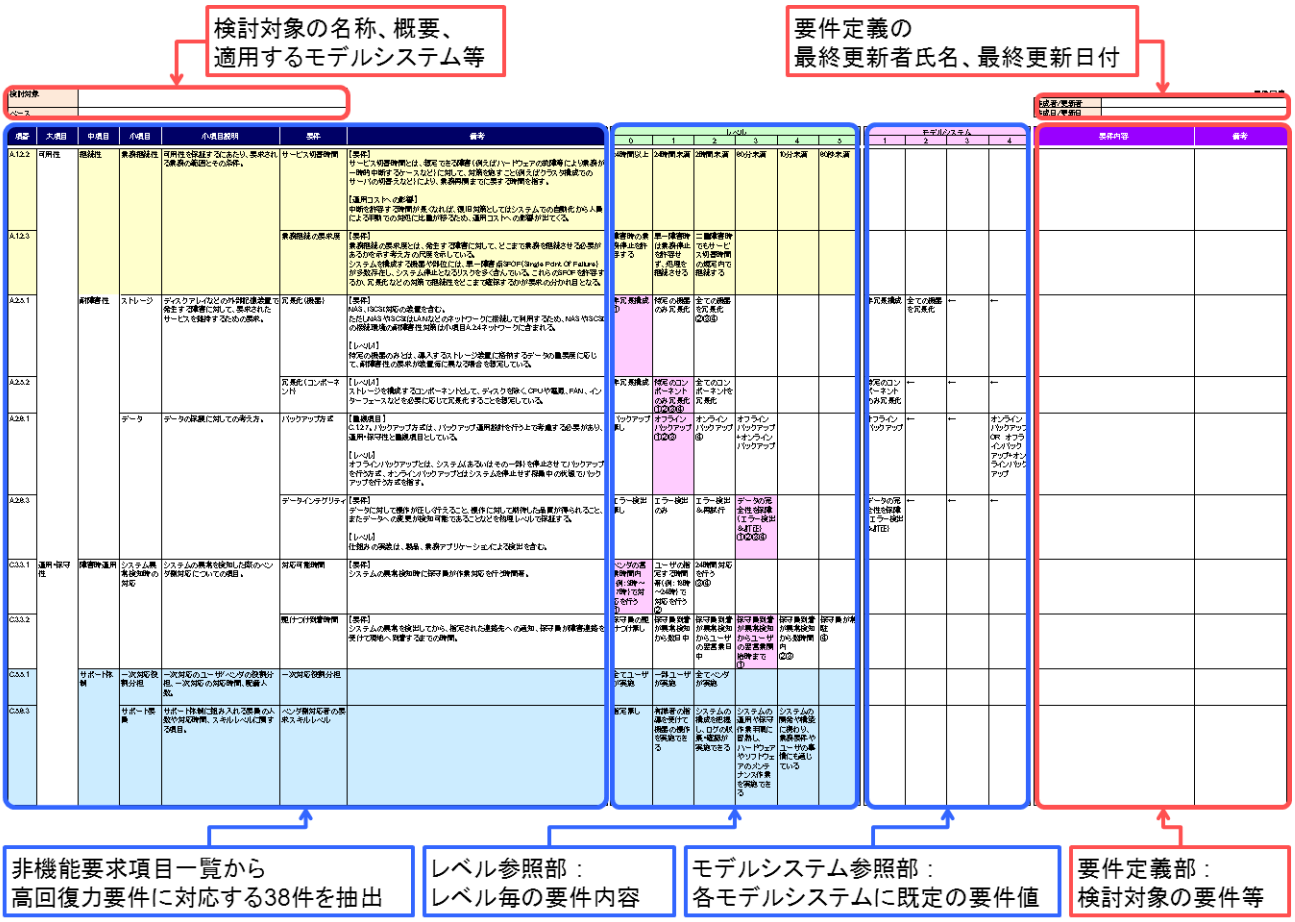


図 4.3.1-1 要件定義ワークシート

ワークシートの構成は 4 部分に大別される。

(1)非機能要求項目表

非機能要求項目一覧から、高回復力要件 37 件に対応する部分を抽出したもの。

(2)レベル参照部

高回復力要件 37 件について、非機能要求項目一覧が持つレベル毎の要件内容を一覧表示する。

(a)前提要件 5 件については、識別のため、すべてのセルに着色(　)している

(b)主要要件 27 件については、高回復力の最小値として、モデル 1 が取るレベルに該当するセルに着色(　)している。

(c)考慮要件 5 件については、識別のため、すべてのセルに着色(　)している。

(3)モデルシステム参照部

主要要件 27 件について、モデルシステム 1～4 に対してあらかじめ設定した要件内容を、一覧表示する。

前提要件および考慮要件については、モデルシステムには内容が設定されていないため、空白が表示される。前提要件はタスク 3.2 要件調整の前段でモデルシステムなどを参考に、考慮要件は同タスクの後段で、それぞれ検討対象独自の内容を設定する。

(4)要件定義部

検討対象が個別に取る要件内容を記入する欄、および備考欄。

備考欄は、要件調整時の覚書、進捗管理などに利用する。

特定の検討対象について要件定義に着手する際に、当該検討対象用のワークシートを生成する。

(1)Excel ブック「要件定義ワークシート」ファイルをダウンロードする。

(2)要件定義作業用に別ファイル名で保存する。

(3)Excel シート「WorkSheet」を元に、検討対象用のコピーを作成する。必要に応じて検討対象毎に別ファイルに保存してもよい。

検討対象用シートは例えば次のように命名する。

<検討対象名>_WorkSheet_<生成日付(yymmss)>

(4)必要な情報を入力する。

表 4.3.1-1 ワークシート生成時に入力すべき項目

項目名	内容	備考
検討対象	検討対象システム基盤の名称、概要など。	検討対象が複数存在する場合には明示することが望ましい。
ベース	検討対象に適用したモデルシステムの番号。	「1」「2」「3」「4」のいずれか。
担当者/更新者	要件検討・定義担当者の氏名	-
作成日/更新日	作成日付	-

4.3.2. タスク 3.2　要件調整

選定したモデルシステムが持つ個々の要件内容が、検討対象(システム基盤)の要件として適切か否か確認し、必要に応じて変更などを加え、要件定義を収斂させる。

例えば目標復旧時間(RTO)について考えると、各モデルシステムの RTO の値は、システム障害時、大規模災害時ともに一定の「幅」を持っている。検討対象の要件を定める際には、ベースに選定したモデルが持つ既定の RTO を、検討対象の「要求」RTO に収斂させる必要がある。
そのために、次のような「調整」作業を行う。

(a)モデルシステムが提示する RTO の「幅」を参考に、検討対象の前提要件を設定する。
(b)RTO と関連する主要要件の内容が、前提要件の内容と整合するよう、必要に応じて変更する。
(c)変更が他の要件の内容に波及するか否かを確認し、影響を受ける要件も併せて変更する。

要件調整の手順は以下の通り。

(1)リスト 3.2.1　調整時の重視・優先事項など確認
経営層および事業部門が何を重視、あるいは優先したいと考えているのか確認する。すなわち、モデルシステムがあらかじめ持つ RTO の「幅」を所期の値に収斂させるのか、あるいは「幅」の下限を遵守する範囲で投資規模を最小化するのか、といった調整の方針を明確化する。

(2)リスト 3.2.2　前提要件の設定
確認された重視・優先事項にしたがい、前提要件を設定する。内容の検討に際し、必要に応じて経営層および事業部門が参画する。決定された内容を「要件内容」欄に記述する。

(3)リスト 3.2.3　主要要件の調整
RTO などの前提要件に寄与すると思われる主要要件について、
・モデルシステムにあらかじめ設定された要件内容がそのまま適用可能か
・あらかじめ設定された要件内容から、非機能要求項目一覧に示された別のレベルの要件内容に変更するのが効果的か
・独自の要件内容を定義する必要があるか
などを検討し、変更結果を「要件内容」欄に記述する。
ひとつの要件に対する変更が契機となり、他の要件の内容を変更する必要が生じていないか、確認しながら作業する必要がある。

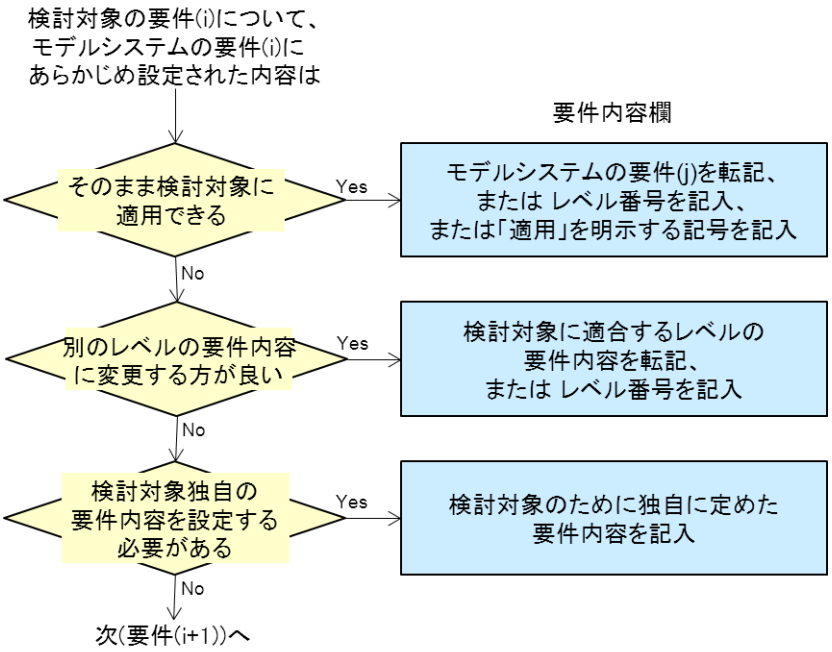


図 4.3.2-1 要件調整の要領

(4)リスト 3.2.4 主要要件調整結果の確認

調整された主要要件の内容が、前提要件の内容と整合していることを確認する。

・整合すればリスト 3.2.5 考慮要件の設定へ

・不整合があればリスト 3.2.3 へ戻り、再調整する

(5)リスト 3.2.5 考慮要件の設定

モデルシステムの特徴には直接影響しない要件であり、「タスク 3 要件定義」における設定は必須ではない。

運用コストなどに影響を与える要件が含まれており、可能な範囲で検討しておくことが望ましい。

(6)リスト 3.2.6 投資規模概算を更新

要件調整の結果として、施設・設備の内容、システム基盤の構成、人的資源などに変更が生じた場合、これに合わせて、モデルシステム選定時に概算した投資規模を算出し直す必要がある。

(7)リスト 3.2.7 調整結果、投資規模概算を確認

情報システム部門担当は調整結果をとりまとめ、経営層および事業部門に報告・説明する。

経営層および事業部門は、調整後の要件内容および投資規模概算が承認できるか否か、意思決定する。

・承認されたらタスク 3.3 要件確定へ

・承認されない場合、(2)調整時の重視・優先事項など確認(リスト 3.2.1)へ戻る

要求 RTO を下げても良いか、どの要件を重点的に検討するかなど、リトライの方針について経営層および事業部門と協議した後、再調整を行う。

要件調整は、必要に応じて、適宜意見・情報などを交換しながら、複数回実施する。

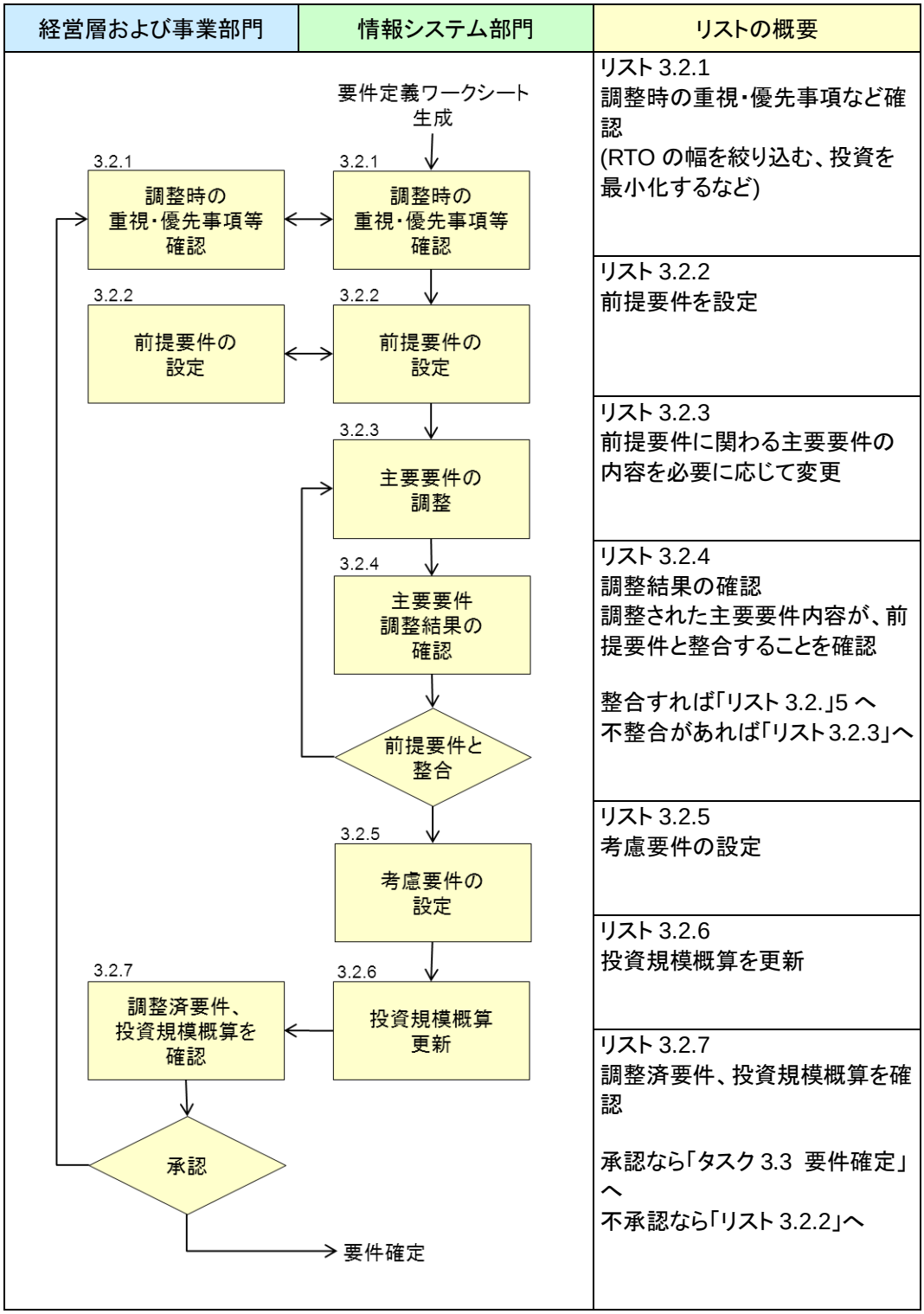


図 4.3.2-2 要件調整の手順

4.3.3. タスク 3.3　要件確定

要件定義ワークシートの必要項目がすべて記入済みであることを確認し、要件定義アクティビティを終了する。

表 4.3.3-1 要件確定時に確認すべき項目

項目名	内容	備考
担当者/更新者	要件定義部の最終更新担当者の氏名	複数名で検討した場合には複数記入しても可。 要件確定時には必須。
作成日/更新日	要件定義部の最終更新日付	要件確定時には必須
要件	当該要件(非機能要求項目)に対して検討対象が取る要件内容の記述。	次のいずれかの記述形式をとる。混在も可。 (1)ベースモデルシステムの要件内容を転記 (2)ベースモデルシステムの要求レベル番号を転記 (3)検討対象に独自の内容を記述 要件確定時には前提要件、主要要件は全項目記入済みであること
備考	要件定義に関する注記	

4.4. アクティビティ 4　導入計画策定

要件定義の結果に基づき、検討対象のシステム基盤を高回復力システム基盤(新システム基盤)として再構築するためのプロジェクトを実施するための導入計画を策定する。
「高回復力システム基盤」であるか否かに関わらず、具体的な導入計画策定に際しては、一般的なシステムライフサイクル管理の枠組にしたがうことが有効であろう。
共通フレーム 2007 や、自社・組織に既定のシステムライフサイクル管理標準があれば、それに準拠することが望ましい。

アクティビティ 4 導入計画策定は、以下のタスクで構成される。

(1)タスク 4.1　ギャップ分析
(2)タスク 4.2　導入計画策定

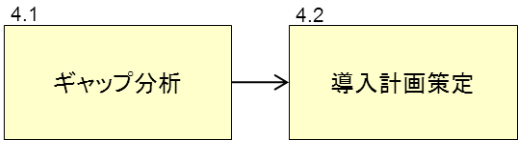


図 4.4-1 導入計画策定の手順

4.4.1. タスク 4.1　ギャップ分析

新システム基盤の要件内容と、現行システム基盤の要件内容の差異を確認し、対策を検討する。
なお新規構築、すなわち現行システム基盤の拡張・更新ではなく、新たなシステム基盤を構築する場合には、「現行システム基盤の要件定義」「ギャップ分析」は必要ない。

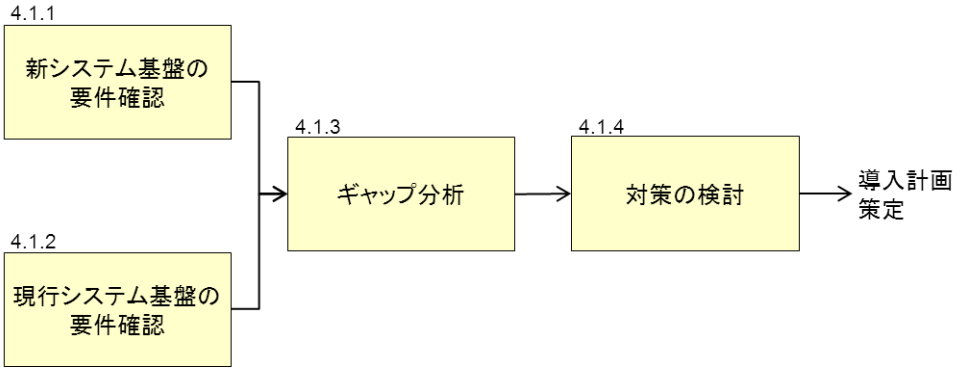


図 4.4.1-1 ギャップ分析の手順

(1)リスト 4.1.1　新システム基盤の要件確認

前項の成果物である、検討対象(システム基盤)の要件定義が確定していることを確認する。

(2)リスト 4.1.2　現行システム基盤の要件確認

検討対象の現状を把握するため、少なくとも前提要件 5 件および主要要件 27 件について、現状の要件内容を確認することが必要である。当該システム基盤構築時などに整備した外部要件定義、仕様書などを利用すると良い。

(3)リスト 4.1.3　ギャップ分析

現行要件内容と新要件内容の差異を分析する。

(4)リスト 4.1.4　対策の定義

(3)で識別された差異を解消するための対策を、システム基盤の構成要素、採用する技術、必要な資源などの観点で整理し、具体的な導入計画を策定するための材料とする。

4.4.2. タスク 4.2　導入計画策定

目的と期待効果、作業手順と成果物、必要な資源、体制とスケジュール、費用などを定め、導入計画を確定する。当該タスクは、「高回復力」であるか否かに関わりなく、一般的なシステムライフサイクル管理の枠組にしたがうものであるため、計画編では説明を省略する。

5. 要件調整における留意点

4 つのモデルシステムでは、非機能要求項目一覧の大項目「可用性」「運用・保守性」「システム環境」に属する要件(非機能要求項目)のうち、主要要件 27 件について、適切と思われる要求レベルがあらかじめ設定されている。
レベルの設定に際しては特に、各モデルシステムが持つ大規模災害時 RTO、大規模システム障害時 RTO の「幅」のうち、最長(最低限度)のものを実現できるようにした。
設定された要件内容は、要件検討および定義の便に供するよう、要件定義ワークシートの「モデルシステム参照部」に一覧表示されている。

5 章では、前提要件 5 件についての説明、主要要件 27 件を調整する際の留意点、予想される影響など、考慮要件 5 件についての説明を述べる。

各要件の見出しは、以下のように構成されている。

<項番> <大項目名> / <中項目名> / <小項目名> / <要件名>

項番 ：	要件の識別番号
大項目 ：	非機能要求を目的、対象範囲の単位でまとめた分類
中項目 ：	非機能要求を検討課題、主題の単位でまとめた分類
小項目 ：	非機能要求の内容を論理的に記述し得る単位
要件 ：	非機能要求の内容を定量的に表現し得る最小単位

5.1. 前提要件

A.1.2.3 可用性 / 継続性 / 業務継続性 / 業務継続の要求度

[要件(非機能要求項目)の説明]

業務継続の要求度とは、発生する障害に対して、どこまで業務を継続させる必要があるかを示す考え方の尺度を示している。

システムを構成する機器や部位には、単一障害点 SPOF（Single Point Of Failure）が多数存在し、システム停止となるリスクを多く含んでいる。これらの SPOF を許容するか、冗長化などの対策で継続性をどこまで確保するかが要求の分かれ目となる。

[要件設定時の留意点]

検討対象システム基盤に対応する業務の重要性などを参考にして設定する。

関連する主要要件の調整時に、次のような検討が必要になる。

・システムの冗長構成をどのようにするか、

・大規模システム障害時の 2 重(多重)障害への対応のためにバックアップサイトで業務継続すべきか。

・大規模災害時に数日以内での業務回復のためにバックアップサイトで業務継続するべきか。

バックアップサイトの設営コストも併せて検討する必要がある。

A.1.3.1 可用性 / 継続性 / 目標復旧水準(業務停止時) / RPO(目標復旧地点)

[要件(非機能要求項目)の説明]

障害、災害などにより業務の中断が発生した時点から見て、最新のバックアップデータが取得された時点。

[要件設定時の留意点]

バックアップ取得時点と中断時点の間隔が短いほど、復旧作業におけるデータリストアは容易になる。各モデルシステムの特徴として明示されてはいないが、RTO に応じて設定できる。

RPO をより最新の値に近づけるためには、バックアップの頻度を高めれば良い。

一方バックアップの頻度を高めるためには、バックアップ時のデータ転送速度、バックアップ用ストレージの容量などを増強する必要があり、コストの増加につながる。

A.1.3.2 可用性 / 継続性 / 目標復旧水準(業務停止時) / RTO(目標復旧時間)

[要件(非機能要求項目)の説明]

大規模システム障害により業務の中断が発生した際、何をどこまで、どれ位で復旧させるかの目標。

[要件設定時の留意点]

情報システムが停止してから業務再開までに要する時間を、モデルシステムの「大規模システム障害時 RTO」を参考に設定する。

「障害時 RTO」を長くすると手作業によるサービス切り替えの必要性が出て来て人的コストが増加する可能性がある、一方「障害時 RTO」を短くするにはシステム冗長化を図ったり、バックアップサイトでのサービス継続の必要性が出てきたりするので設備への投資を考慮する必要がある。

A.1.3.3 可用性 / 継続性 / 目標復旧水準(業務停止時) / RLO(目標復旧レベル)

[要件(非機能要求項目)の説明]

業務の中断が発生した際、何を復旧の対象とするかのレベルを示す。

「レベル 0 システムの復旧」とは、ハードウェアの復旧だけでなくデータのリストアまでを対象とする。

「レベル 1 特定業務のみ」とは、例えば A.1.2.1 対象業務範囲で定義する継続性が要求される業務などを指す。

[要件設定時の留意点]

RLO は代替機やバックアップサイトの機器などの性能に直接影響するので、大規模システム障害時や大規模災害時のあるべき業務の質や量を想定しつつ、投資額との関係を十分考慮して調整する必要がある。

「A.1.3.2 可用性 / 継続性 / 目標復旧水準(業務停止時) / RTO(目標復旧時間)」との関連に注意すること。

A.1.4.1 可用性 / 継続性 / 目標復旧水準 / システム再開目標

[要件(非機能要求項目)の説明]

大規模災害により情報システムが停止、業務が中断してから、業務再開までに要する時間を指す。

[要件設定時の留意点]

モデルシステムの特徴「大規模災害時 RTO」を参考に設定する。

大規模災害時の RTO を短くするためにはバックアップサイトでの業務回復を図る必要があるため、バックアップサイトの設備や要員の確保のコストを考慮する必要がある。

5.2. 主要要件

5.2.1. 可用性

可用性は、情報システムを継続的に利用可能とするための要求である。情報システムは何事も問題なく継続できることが望ましい。障害、災害など、様々な要因による、予期せぬ停止を発生させないようにするため、あるいは停止が発生したとしても影響範囲を極小化し、情報システムの稼働品質を保証するために必要な事項が検討、定義の対象である。

A.2.1.1 可用性 / 耐障害性 / サーバ / 冗長化(機器)

[要件(非機能要求項目)の説明]

「機器の冗長化」とは筐体を複数用意することによる冗長化を指す。

「レベル 1 特定のサーバで冗長化」とは、システムを構成するサーバの種別（DB サーバや AP サーバ、監視サーバなど）で冗長化の対応を分けることを意味する。

また要求としてサーバの単位ではなく、業務や機能の単位で冗長化を指定する場合、それを実装するサーバを想定してレベルを設定する。

サーバを冗長化することは、処理系の耐障害性を高める上で有効だが、同一サイトに設置されている限り、大規模災害からの回復力向上に大きく寄与するものではない。

[要件調整時の留意点]

大規模システム障害時の RTO に影響を与える。一方、冗長構成により設備のコストを考慮する必要が出てくる。具体的には、大規模災害に備えるために、バックアップサイト設営及びサーバ設置、またクラウドサービスの利用などを考慮する必要がある。

「A.2.3.1 可用性 / 耐障害性 / ネットワーク機器 / 冗長化(機器)」、

「A.2.5.1 可用性 / 耐障害性 / ストレージ / 冗長化(機器)」との関連に注意すること。

A.2.1.2 可用性 / 耐障害性 / サーバ / 冗長化(コンポーネント)

[要件(非機能要求項目)の説明]

「レベル 1 特定のコンポーネントのみ冗長化」とは、サーバを構成するコンポーネントとして、内蔵ディスクや、電源、ファンなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのミラー化や、ネットワーク IF カードの冗長化など）。

各モデルシステムでは共通の前提として特定のコンポーネントが冗長化されているものとしている。

サーバのコンポーネントを冗長化することは、サーバ単体の耐障害性を高める上で有効だが、大規模災害からの回復力向上に大きく寄与するものではない。

モデルシステム 1 では、メインサイトのサーバ単体の稼働率が、システム全体の稼働率に直結するため、単体レベルの耐障害性を高めておくことには意義がある。

[要件調整時の留意点]

「特定のコンポーネント」を具体的に特定することにより、サーバ単体の価格、運用コストなどの積算精度が向上する。その場合は、「A.1.2.3 可用性 / 継続性 / 業務継続性 / 業務継続の要求度」の観点から、情報システムの停止許容時間と、システム構成から単一障害点がないことなどの確認を行うこと

A.2.3.1 可用性 / 耐障害性 / ネットワーク機器 / 冗長化(機器)

[要件(非機能要求項目)の説明]

ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。

「レベル 1 特定の機器のみ冗長化」とは、ネットワークを構成するルータやスイッチの内、冗長化したサーバを収容するスイッチなどを想定している。

[要件調整時の留意点]

大規模システム障害時の RTO に影響を与える。一方、冗長構成により設備のコストを考慮する必要が出てくる。

「A.2.1.1 可用性 / 耐障害性 / サーバ / 冗長化(機器)」、

「A.2.5.1 可用性 / 耐障害性 / ストレージ / 冗長化(機器)」、との関連に注意すること。

A.2.3.2 可用性 / 耐障害性 / ネットワーク機器 / 冗長化(コンポーネント)

[要件(非機能要求項目)の説明]

ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。

「レベル 1 特定のコンポーネントのみ冗長化」とは、ネットワーク機器を構成するコンポーネントとして、電源や CPU、ファンなどを必要に応じて冗長化することを想定している。

各モデルシステムでは共通の前提として特定のコンポーネントが冗長化されているものとしている。

ネットワーク機器のコンポーネントを冗長化することは、機器単体の耐障害性を高める上で有効だが、大規模災害からの回復力向上に大きく寄与するものではない。

モデルシステム 1 では、メインサイトのネットワーク機器の稼働率が、システム全体の稼働率に直結するため、単体レベルの耐障害性を高めておくことには意義がある。

[要件調整時の留意点]

「特定のコンポーネント」を具体的に特定することにより、ネットワーク機器単体の価格、運用コストなどの積算精度が向上する。

サーバのコンポーネントあるいは機器の冗長化との組み合わせで耐障害性を高める組み合わせが種々考えられるので、コストや RTO の観点から考慮すること。その場合は、「A.1.2.3 可用性 / 継続性 / 業務継続性 / 業務継続の要求度」の観点から、業務システム毎に停止許容時間と、システム構成から単一障害点がないことなどの確認を行うこと。

A.2.4.1 可用性 / 耐障害性 / ネットワーク / 回線の冗長化

[要件(非機能要求項目)の説明] 物理的な伝送路を冗長化すること。

「回線の冗長化」とは、ネットワークを構成する伝送路（例えば LAN ケーブルなど）を物理的に複数用意し、一方の伝送路で障害が発生しても他方での通信が可能な状態にすること。

「レベル 1 一部冗長化」とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。

[要件調整時の留意点]

回線の冗長化により、耐障害性は向上する。一方、冗長構成をとることにより設備コストが増加することを

考慮する必要がある。「A.2.4.2 可用性 / 耐障害性 / ネットワーク / 経路の冗長化」との組み合わせで大規模システム障害時への耐障害性を考慮すること。
メインサイト内における措置だけでは、大規模災害からの回復力向上に大きく寄与するものではない。
モデルシステム 3、4 のようにバックアップサイトを備える場合には、メインサイトとバックアップサイトを接続する外部ネットワークの冗長化を考慮する必要がある。

A.2.4.2 可用性 / 耐障害性 / ネットワーク / 経路の冗長化

[要件(非機能要求項目)の説明]

「経路の冗長化」とは、ネットワーク内でデータを送受信する対象間で、データの流れる順序（経由するルータの順序）を複数設定することで、ある区間で障害が発生しても、他の経路で迂回し通信を可能な状態にすること。
「レベル 1 一部冗長化」とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。

[要件調整時の留意点]

経路の冗長化により耐障害性は向上する。一方、冗長構成をとることによるコストへの影響も考慮する必要がある。具体的には「A.2.4.1 可用性 / 耐障害性 / ネットワーク / 回線の冗長化」との組み合わせにより大規模システム障害時への耐障害性を考慮すること。
メインサイト内における措置だけでは、大規模災害からの回復力向上に大きく寄与するものではない。

A.2.5.1 可用性 / 耐障害性 / ストレージ / 冗長化(機器)

[要件(非機能要求項目)の説明]

ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求。
「レベル 1 特定の機器のみ冗長化」とは、導入するストレージに格納するデータの重要度に応じて、耐障害性の要求が装置毎に異なる場合を想定している。
ストレージを冗長化することは、性能向上および耐障害性向上のために有効だが、同一サイトに設置されている限り、大規模災害からの回復力向上に大きく寄与するものではない。

[要件調整時の留意点]

ストレージの冗長化により耐障害性は向上する。一方、冗長構成をとることにより設備コストが増加することを考慮する必要がある。
「A.2.1.1 可用性 / 耐障害性 / サーバ / 冗長化(機器)」、
「A.2.3.1 可用性 / 耐障害性 / ネットワーク機器 / 冗長化(機器)」との関連に注意すること。

A.2.5.2 可用性 / 耐障害性 / ストレージ / 冗長化(コンポーネント)

[要件(非機能要求項目)の説明]

「レベル 1 特定のコンポーネントのみ冗長化」とは、ストレージを構成するコンポーネントとして、ディスクを除く、CPU や電源、ファン、インターフェースなどを必要に応じて冗長化することを想定している。
各モデルシステムでは共通の前提として特定のコンポーネントが冗長化されているものとしている。
ストレージのコンポーネントを冗長化することは、機器単体の耐障害性を高める上で有効だが、大規模災

害からの回復力向上に大きく寄与するものではない。
モデルシステム 1 では、メインサイトのストレージ単体の稼働率が、システム全体の稼働率に直結するため、単体レベルの耐障害性を高めておくことには意義がある。

[要件調整時の留意点]

「特定のコンポーネント」を具体的に特定することにより、機器単体の価格、運用コストなどの積算精度が向上する。その場合は、「A.1.2.3 可用性 / 継続性 / 業務継続性 / 業務継続の要求度」の観点から、業務システムの停止許容時間と、システム構成から単一障害点がないことなどの確認を行うこと。

A.2.5.3 可用性 / 耐障害性 / ストレージ / 冗長化(ディスク)

[要件(非機能要求項目)の説明]

「レベル 1 RAID5 による冗長化」「レベル 2 RAID1 による冗長化」では、性能上の要求から RAID0 との組み合わせを検討する。

[要件調整時の留意点]

モデルシステムではディスクの RAID 構成での冗長化を想定しているが、「A.2.5.1 ストレージの冗長化」との組み合わせで耐障害性を高める組み合わせが種々考えられるので、コストや RTO の観点から考慮すること。

A.2.6.1 可用性 / 耐障害性 / データ / バックアップ方式

[要件(非機能要求項目)の説明]

オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式、
オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。
各モデルシステムにおけるバックアップの保有形態とバックアップ方式の組合せについて、各モデルシステムとの関係も含め、下表に示す。

	オンライン	オフライン
同期バックアップ	可能(モデルシステム 4)	不可能
非同期バックアップ	可能(モデルシステム 3)	可能(モデルシステム 1、2、3)

[要件調整時の留意点]

バックアップ方式は、目標 RTO/RPO を満足するよう、選定される必要がある。

A.2.6.3 可用性 / 耐障害性 / データ / データインテグリティ

[要件(非機能要求項目)の説明]

データの保護に対しての考え方。
データに対して操作が正しく行えること、操作に対して期待した品質が得られること、またデータへの変更が検知可能であることなどを保証する。仕組みの実装は、製品、業務アプリケーションによる検出を含む。

[要件調整時の留意点]

モデルシステムではリカバリー時のデータの完全性を必須としている。

A.3.1.1 可用性 / 災害対策 / システム / 復旧方針

[要件(非機能要求項目)の説明]

地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすため、大規模災害のための代替の機器として、どこに何が必要かを決める項目。

レベル 1 および 3 の「限定された構成」とは、復旧する目標に応じて必要となる構成（例えば、冗長化の構成は省くなど）を意味する。

レベル 2 および 4 の「同一の構成」とは、復旧後も復旧前と同じサービスレベルを維持するため、本番環境と同一のシステム構成を必要とすることを意味する。

[要件調整時の留意点]

モデルシステム 1、2 では遠隔地（クラウドやデータセンターなど）に保管したデータなどを利用して復旧することを想定している。

モデルシステム 3、4 では、バックアップサイトにおいて業務を継続することを想定している。

A.3.2.1 可用性 / 災害対策 / 外部保管データ / 保管場所分散度

[要件(非機能要求項目)の説明]

地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するなどの要求。

大規模災害などにより、データが失われることがないよう、バックアップを遠隔地に保管することが最低限必要である。

[要件調整時の留意点]

モデルシステムでは、データ・プログラムのメディアなどへの保管、バックアップサイトへの保管、いずれの場合も、少なくとも 1 個所の遠隔地に保管するものとしている。

A.3.2.2 可用性 / 災害対策 / 外部保管データ / 保管方法

[要件(非機能要求項目)の説明]

地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するなどの要求。

媒体の種類や保管方法に関わりなく、必要なデータが保全されていることが重要である。

クラウド上のストレージを利用することも選択肢となり得る。

[要件調整時の留意点]

モデルシステム 1、2 ではデータやプログラムのバックアップを遠隔地（データ保管倉庫やクラウドのストレージサービスなど）に保管する。

モデルシステム 3、4 では、バックアップサイトにおいて業務を継続するため、当該バックアップサイトにデータやプログラムのバックアップを保管する。

5.2.2. 運用・保守性

運用・保守性は、システムの運用と保守のサービスに関する要求である。運用や保守に関する要求項目は、システムの運用方法や管理者の作業手順を決定するものであり、「必要なバックアップがとられておらず、障害からの復旧ができない」といったトラブルを引き起こすことのないよう、要件定義の段階で十分に検討しておく必要がある。

C.1.3.1 運用・保守性 / 通常運用 / 運用監視 / 監視情報

[要件(非機能要求項目)の説明]

システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する要件。セキュリティ監視については本項目には含まれない。

監視とは情報収集を行った結果に応じて適切な宛先に通知することを意味する。

(a)死活監視とは、対象のステータスがオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。

(b)エラー監視とは、対象が出力するログなどにエラー出力が含まれているかどうかを判断する監視のこと。トレース情報を含む場合は、どのモジュールでエラーが発生しているのか詳細についても判断することができる。

(c)リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて CPU やメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。

(d)パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスク I/O、ネットワーク転送などの応答時間やスループットについて判断する監視のこと。

エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、システムの品質を維持するための運用コストが下がる。

[要件調整時の留意点]

監視情報のレベルを高めればそれだけ障害部位の特定精度が高まるが、運用負荷が高くなる。

モデルシステムでは最低限の想定をしているので、障害部位の特定時間を短縮したい場合は、より高い要求レベルに変更する。

必要に応じて、以下のような監視対象について、それぞれのレベルを設定する。

・システムの監視
・プロセスの監視
・データベースの監視
・ストレージの監視
・サーバ(ノード)の監視
・端末/ネットワーク機器の監視
・ネットワーク・パケットの監視

C.1.3.2 運用・保守性 / 通常運用 / 運用監視 / 監視間隔

[要件(非機能要求項目)の説明]

各モデルの障害時 RTO(目標回復時間)から見て、モデル 1・2 では 5 分間隔程度、モデル 3・4 では数回/分以上の頻度で確認する必要がある。

[要件調整時の留意点]

監視間隔を短くすれば、それだけ早く障害を検知できる可能性が高まるが、その分監視用のトラフィックが増えてネットワークを圧迫することを考慮すること。

「A1.2.2 可用性 / 継続性 / 業務継続性 / サービス切替時間」との関連に注意すること。

C.2.5.1 運用・保守性 / 保守運用 / 定期保守頻度 / 定期保守頻度

[要件(非機能要求項目)の説明]

システムの保全に必要なハードウェア、ソフトウェア定期保守作業の実施頻度。

[要件調整時]の留意点

定期保守の頻度を高くすれば、保守対象機器の障害発生を未然に防ぐ可能性が高まることが期待できる。その場合、保守のコストが高くなることを考慮に入れたうえで調整すること。

C.2.6.1 運用・保守性 / 保守運用 / 予防保守レベル / 予防保守レベル

[要件(非機能要求項目)の説明]

システム構成部材が故障に至る前に予兆を検出し、事前交換などの対応をとる保守の実施頻度。

[要件調整時の留意点]

予兆検出・保守の頻度を高くすれば、保守対象機器の障害発生を未然に防ぐ可能性が高まることが期待できる。その場合、保守のコストが高くなることを考慮に入れたうえで調整すること。

C.3.2.1 運用・保守性/ 障害時運用 / 障害復旧自動化の範囲 / 障害復旧自動化の範囲

[要件(非機能要求項目)の説明]

障害復旧に関するオペレーションを自動化する範囲に関する要件。

「一部の障害復旧作業」とは、特定パターン（あるいは部位）の障害復旧作業に関してのみ自動化を行うようなケースを指す。

[要件調整時の留意点]

障害発生時の復旧時間（RTO）を短くできるが、自動化のための開発コストが発生する。運用コスト軽減の期待効果とのバランスを考慮して、適用可能性を検討すること。

C.3.3.1 運用・保守性/ 障害時運用 / システム異常検知時の対応 / 対応可能時間

[要件(非機能要求項目)の説明]

システムの異常検知時に保守員が作業対応を行う時間帯。

[要件調整時の留意点]

対応時間帯を広くすれば障害発生時の復旧時間（RTO）を短くできる。一方、外部ベンダを利用する場合には、保守のコストが高くなることを考慮し調整すること。

C.3.3.2 運用・保守性/ 障害時運用 / システム異常検知時の対応 / 駆けつけ到着時間

[要件(非機能要求項目)の説明]

システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着す

るまでの時間。

[要件調整時の留意点]

モデル 4 の場合、メインサイト、バックアップサイト共に「常駐」する必要がある。

このため、運用のための設備や体制への人的資源コストを考慮する必要が出てくる。平常時の作業も含め、コストと効果の比較検討を行うこと。

C.3.3.3 運用・保守性/ 障害時運用 / システム異常検知時の対応 / SE 到着平均時間

[要件(非機能要求項目)の説明]

システム異常を検知してから SE が到着するまでの平均時間。

[要件調整時の留意点]

モデル 4 の場合、メインサイト、バックアップサイト共に「常駐」する必要がある。

このため、運用のための設備や体制への人的資源コストを考慮する必要が出てくる。平常時の作業も含め、コストと効果の比較検討を行うこと。

C.3.4.1 運用・保守性/ 障害時運用 / 交換用部材の確保 / 保守部品確保レベル

[要件(非機能要求項目)の説明]

障害の発生したコンポーネントに対する交換部材の確保方法。

当該システムに関する保守部品の確保レベル。

[要件調整時の留意点]

障害発生時の復旧時間（RTO）により自社内での確保も想定すること。部品により確保が困難な場合もあり得るので注意すること。

C.3.4.2 運用・保守性/ 障害時運用 / 交換用部材の確保 / 予備機の有無

[要件(非機能要求項目)の説明]

障害の発生したコンポーネントに対する交換部材の確保方法。

予備機の用意の有無。用意しないか、一部または全部用意するかを定める。

[要件調整時の留意点]

メインサイトにおける冗長化された処理系、バックアップサイトの待機システムなどを「予備」とみなすことはしない。

コストへの影響を考慮すること。

「C.3.4.1 運用・保守性/ 障害時運用 / 交換用部材の確保 / 保守部品確保レベル」との関連に注意すること。

C.4.3.1 運用・保守性/ 運用環境 / マニュアル準備レベル / マニュアル準備レベル

[要件(非機能要求項目)の説明]

運用のためのマニュアルの準備のレベル。

通常運用のマニュアルには、システム基盤に対する通常時の運用（起動・停止など）に関わる操作や機能についての説明が記載される。

保守運用のマニュアルには、システム基盤に対する保守作業（部品交換やデータ復旧手順など）に関わる操作や機能についての説明が記載される。

障害発生時の一次対応に関する記述（系切り替え作業やログ収集作業など）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。

ユーザの運用に合わせたカスタマイズされたマニュアルを作成することは、導入コストを増大させる一方、ユーザが運用時に手順を調査する負担が減少するため運用コストは減少すると考えられる。

「高回復力」の観点からは、障害・災害時を想定して、担当者以外にも理解できて、必要最低限の対処を行えるような「解りやすい」マニュアルを整備できると良い。

[要件調整時の留意点]

障害発生時に本来の担当者が対応できない場合も想定し、事前に訓練を受けていない者でも、最低限の対処ができる内容を目標とすること。非常時を想定した訓練の内容・頻度についても検討すること。

5.2.3. システム環境

システム環境とは、システムの設置環境に関する要求である。設置環境は、容易には変更することが困難であり、要件定義の漏れが大きな手戻りなどにつながる場合もあるため重要な項目である。

F.4.1.1 システム環境 / 機材設置環境条件 / 耐震/免震 / 耐震震度

[要件(非機能要求項目)の説明]

地震発生時にシステム設置環境で耐える必要のある実効的な最大震度を規定。

モデルシステムでは、機材設置環境においては、特別な免震装置などはなく、屋外の振動がそのまま建屋に伝わると想定している。すなわち、外部の震度と設置環境の震度は一致すると考えてレベルを設定している。

[要件調整時の留意点]

高回復力システム基盤においては震度「6 強」以上の地震発生時、メインサイトは「停止」し、バックアップサイトにより業務/システム運用を「再開」するものと想定している。

(モデルシステム 1、2 はメインサイトの復旧を待って遠隔地へ退避させたバックアップデータをリストアする)

F.4.4.4 システム環境 / 機材設置環境条件 / 電気設備適合性 / 停電対策

[要件(非機能要求項目)の説明]

機器の設置場所において、停電時にどの程度の期間にわたり電源供給が必要かについての要件。移行時の並行稼動が可能か否かについても確認が必要である。可能であれば事前確認を実施する。

要求される電源供給時間のレベルにしたがって、UPS, CVCF など電源安定化の対策を検討する。

[要件調整時の留意点]

各モデルシステムでは、大規模災害時に外部からの電力供給が断たれた場合に、情報システムが安全に停止できるのに必要な時間を設定している。

停電対策のレベルは、耐障害性(障害時対応)のみでなく、大規模災害時 RTO も考慮して検討すること。

5.3. 考慮要件

C.5.5.1 運用・保守性 / サポート体制 / 一次対応役割分担 / 一次対応役割分担

[要件(非機能要求項目)の説明]

一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数。

レベルの設定はユーザ/ベンダの分担比率のみを基準にしているように見えるが、重要なのは「一次対応」局面において必要な役割、責任、スキルレベル、員数などを明らかにし、個人が特定可能なレベルで「担当者」を定めることである。

運用計画策定時に検討しておくことを推奨する。

C.5.6.3 運用・保守性 / サポート体制 / サポート要員/ ベンダ側対応者の要求スキルレベル

[要件(非機能要求項目)の説明]

サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する要件。

運用計画策定時に人員調達方法、定期的な訓練計画などを策定しておくことを推奨する。

C.5.8.2 運用・保守性 / サポート体制 / オペレーション訓練 / オペレーション訓練範囲

[要件(非機能要求項目)の説明]

オペレーション訓練実施に関する要件。

「通常運用」とは、システム基盤に対する通常時の運用(起動・停止など)に関わる操作を指す。「保守運用」とは、システム基盤に対する保守作業(部品交換やデータ復旧手順など)に関わる操作を指す。

高回復力システム基盤では、確実に復旧作業を遂行できるよう、定期的に訓練を実施しておくことが重要である。

運用計画策定時に定期的な訓練計画を策定しておくことを推奨する。

C.5.9.1 運用・保守性 / サポート体制 / 定期報告会 / 定期報告会実施頻度

[要件(非機能要求項目)の説明]

保守に関する定期報告会の開催の要否。

障害発生時に実施される不定期の報告会は本メトリクスには含まない。

高回復力システム基盤では、障害発生時の円滑かつ迅速な対応につながるよう、定期的にコミュニケーションを取ることが重要である。

C.5.9.2 運用・保守性 / サポート体制 / 定期報告会 / 報告内容のレベル

[要件(非機能要求項目)の説明]

保守に関する定期報告会において、報告内容に含められる事項。

高回復力システム基盤では、障害を未然に防ぐ観点から、改善提案を含めた報告レベルを強く推奨する。