システム要件定義成果物サンプル＆ガイド
DS-301 ： 可用性要件定義

第1.10版

2018年08月29日

１．概要

システムを継続的に利用可能とするための要求を整理し、指標を設定して実現水準を明確にする。

２．使途

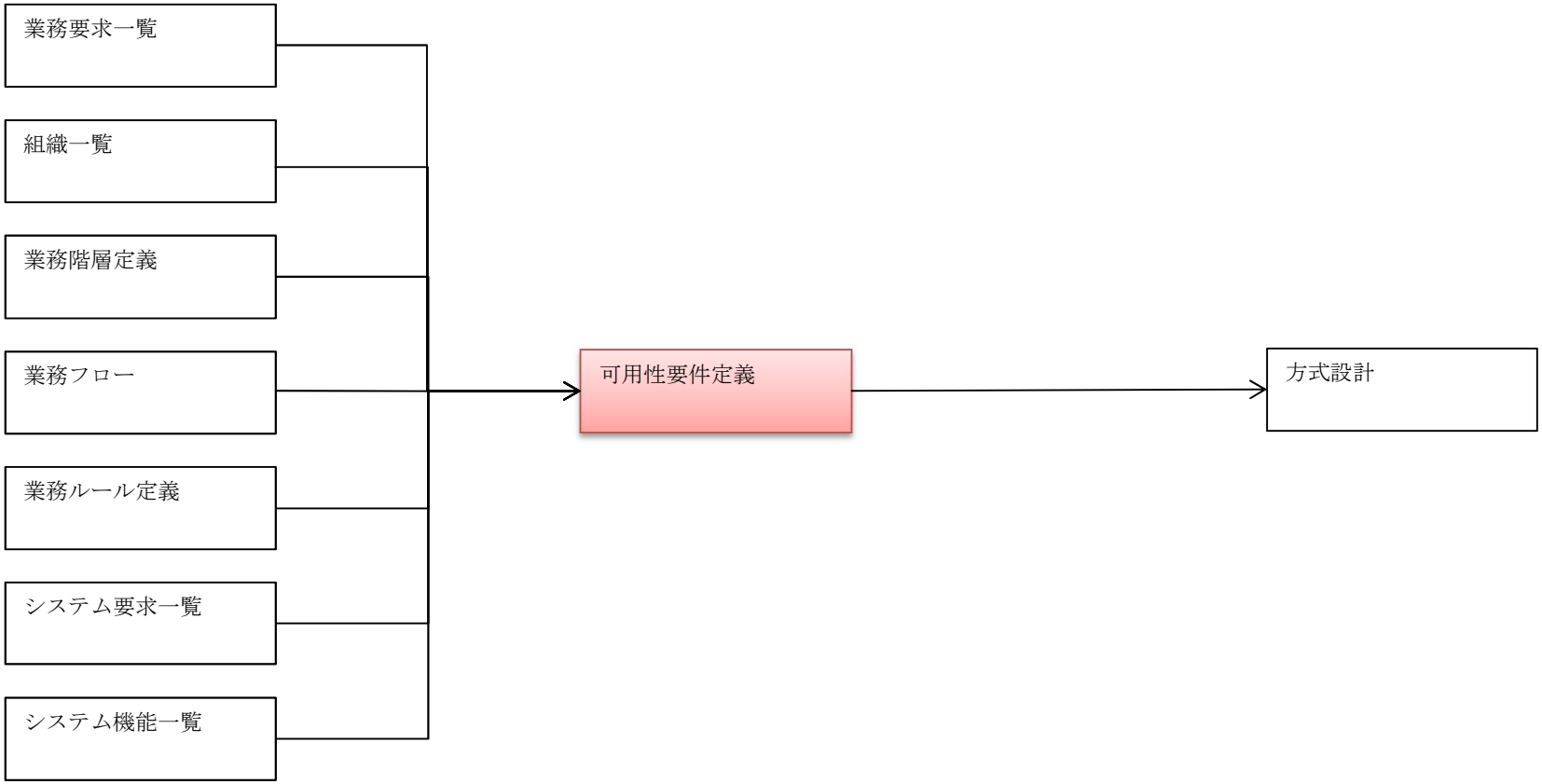
● システムを継続的に利用可能とするために、実現する必要がある事項について指標を設定し方式設計（サイジング等）のインプットとする。

３．記入要領

No	記述内容 (SX-XX-XXは、関連するプロセスIDを指す。)		記述内容説明	補足
1	継続性 S3-02-01	1.1 業務継続性	継続した稼働を保証する業務の対象範囲、障害発生時の業務再開までの条件を記述する。	
2	目標復旧水準 S3-02-02	2.1 目標復旧水準（業務停止）	業務停止を伴う障害が発生した場合の復旧までの目標水準を記述する。	
		2.2 目標復旧水準 (大規模災害時)	大規模災害発生時の復旧までの目標水準を記述する。	
3	稼働率 S3-02-03	3.1 稼働率	明示された利用条件の下で、業務継続性を保証したシステムが要求されたサービスを提供できる割合を記述する。	
4	災害対策 S3-02-04	4.1 システム	大規模災害発生を想定し、業務を継続するためのシステム復旧方針について記述する。	
		4.2 外部保管データ	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に保管するなどの要求を記述する。	
		4.3 付帯設備	各種災害を想定して、システムの付帯設備への要求を記述する。	
5	耐障害性 S3-02-05	5.1 サーバ	システムを構成するサーバ機器、コンポーネントについて、障害時にサービスを維持するための要求を記述する。	
		5.2 ネットワーク機器	ルータやスイッチなどネットワークを構成する機器、コンポーネントについて、障害時にサービスを維持するための要求を記述する。	
		5.3 ストレージ	ディスクアレイなど外部記憶装置について、障害時にサービスを維持するための要求を記述する。	
		5.4 端末	パソコンなど端末装置について、障害時にサービスを維持するための要求を記述する。	
		5.5 ネットワーク	ネットワークの信頼性を向上させるための要求を記述する。	

[IPA/SEC『非機能要求グレード：システム基盤の非機能要求に関する項目一覧』[5]より引用、一部改訂]

４．他成果物との関係


業務要求一覧
組織一覧
業務階層定義
業務フロー
業務ルール定義
システム要求一覧
システム機能一覧
可用性要件定義
方式設計

５．表記例

１.継続性

１．１．　業務継続性

本システムの可用性を定めるにあたり、対象業務範囲と業務継続の条件を定義する。

対象業務	システム利用停止から再開までの所要時間	決定理由・根拠	備考
オンライン機能	５分以内にサービス再開できること	左記時間を超えると販売機会損失となる為	オンラインWeb、非同期処理を含む
データ連携機能	５分以内にサービス再開できること	左記時間を超えると販売機会損失となる為	
バッチ処理機能	８時間以内にジョブ実行が再開できること	左記時間を超えると日報集計が不能となる為	

※多重障害(複数コンポーネントの同時故障)における切替時間は定めない。

※サービス再開とは受注入力、売上照会などの主要業務が正常に運用できる状態を言う。マスタメンテなどの付帯機能は含まない。

２.目標復旧水準

２．１.目標復旧水準（業務停止）

１）　目標復旧地点（どの時点までデータ復旧するか）は次の通りとする。

①　障害発生直前にコミット完了したトランザクションまで復旧可能であること。

２）　目標復旧時間（データ復旧に許容する所要時間）は次の通りとする。

No	対象機能	目標復旧時間	説明
1	オンライン機能	３時間	復旧作業開始から、再びシステム利用が可能になるまでの時間
2	データ連携機能	３時間	復旧作業開始から、再びシステム利用が可能になるまでの時間
3	バッチ処理機能	２時間	復旧作業開始から、ジョブ再実行可能状態になるまでの時間

※ハードウェア交換が伴う作業の場合、ハード交換完了までの時間は含まない(別途保守要件で定義)

３）　目標復旧レベル（何を復旧の対象とするか)は次の通りとする。

①　全ての業務を稼動させる。

２．２.目標復旧水準（大規模災害時）

１）　大規模災害時のシステム再開目標

①　大規模災害が発生しコンピュータルーム内のサーバ類が利用不能となった場合に、復旧（ＤＲへの切替）期間は２週間を想定する。

3.稼働率

3．1.稼働率

1） 本システムの稼働率(システムが要求されたサービスを提供できる割合)目標を次の通り定義する。

No	対象機能	稼働率目標値	説明
1	オンライン機能	９９．９９％	１日の稼働時間を１６．５時間(０６：３０～２３：００)、年間稼動日を３６３日(３６５－年末年始)とした場合、年間の業務中断時間は約３６分間となる。
2	データ連携機能	９９．９９％	２４時間、３６３日稼動とした場合、年間の業務中断時間は約５２分間となる。
3	バッチ処理機能	９９．９９％	１日の稼働時間を６．５時間(０：００～０６：３０）、年間稼働日を３６３日とした場合、年間の業務中断時間は約１４分間となる。

4.災害対策

4．1.システム

1） 本システムの災害時の復旧方針は次の通りとする。

① 本番環境と同一構成のシステムをＤＲサイトに復旧させ以下のシステムを稼動させる。

- 営業システム
- 財務会計システム

4．2.外部保管データ

1） データセンターの大規模被災を想定し、以下の対策を実施する。

① 保護対象データ … 本番データベースのデータ

② 対策方法 … 保護対象データを保管したテープカートリッジを遠隔地に搬送する。

③ 実施周期 … 週次(１週間のうち、特定曜日のバックアップデータを遠隔地に搬送する)

④ 目標復旧地点 … 週次のフルバックアップ取得時点(特定曜日の夜間バッチ終了時点)

4．3.付帯設備

1） 各種災害に対する付帯設備の対策は次の通りとする。

① データセンターで利用する当業務用のラックとして4ラック（700W×1000D×2000H）が割当可能とする。

② 電源については相当量が確保されている。

5．耐障害性

耐障害性（S3-02-05）
⇒ サンプル提供なし