高回復力システム基盤導入ガイド

事例編

2012 年 7 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

Copyright © 2012 IPA, All Rights Reserved

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でも事業活動を継続し、また万が一中断した場合においても事業活動を迅速に再開するうえで、情報システムは重要な要素のひとつである。事業活動の継続および迅速な再開には、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対策の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 7 月	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手順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。

※事例編を読む前に、概要編や計画編を読むことを推奨する。

Copyright © 2012 IPA, All Rights Reserved

1.3. 事例編の概要

1.3.1. 事例編の主要な内容

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解説するために、主に下表に示すような内容からなる。

表 1.3.1-1　事例編の主要な内容

主要な内容	説明
企業や地方公共団体(以下、各組織という)における対策事例に基づく参考となる情報や留意点	「情報システム基盤の復旧に関する対策の調査」で実施したアンケート調査、ヒアリング調査(事例調査)の結果をもとに、計画編で示している高回復力システム基盤の導入手順や要件を基準として分析等を行った結果と各社事例について、紹介する。 ・導入手順の観点でのポイント ・要件の観点でのポイント ・各組織の対策事例
高回復力システム基盤構築におけるクラウドサービスの活用について	コスト(投資)面の制約により高回復力システム基盤構築への取り組みが難しいと考えている組織にとって、クラウドサービスの活用は有用な選択肢となっている。高回復力システム基盤導入の観点からクラウドサービスの活用に関する以下の内容について紹介する。 ・高回復力システム基盤導入に有用なクラウドサービスの概要 ・高回復力システム基盤導入におけるクラウドサービス利用の留意点

1.3.2. 掲載している事例について

事例編は「情報システム基盤の復旧に関する対策の調査」で実施したアンケート調査、ヒアリング調査(事例調査)の結果をもとに作成している。「情報システム基盤の復旧に関する対策の調査」については、「情報システム基盤の復旧に関する対策の調査報告書」(http://sec.ipa.go.jp/reports/20120725.html)を参照していただきたい。

ヒアリング調査の概要を下表に示す。なお表中の「ITガバナンス」は、ITの構築・運用等に関する狭義の「統制」の意味で用いられている。

表 1.3.2-1 ヒアリング調査の概要

項目	内容		
調査目的	システム復旧対策を実施している組織におけるITサービス継続マネジメントや具体的な対策の内容等を調査し、組織がITサービス継続の取り組みを検討・実施する際の参考となる資料を得ることを目的とする。		
調査対象	バックアップやシステムの冗長化、バックアップサイトの構築等のシステム復旧対策を実施している企業や地方公共団体 10 組織		
調査項目	①事業の特徴とIT	組織のITの活用状況やITガバナンスの取り組み	業種・組織概要
			全社レベルのITガバナンス
			BCP（事業継続計画）の策定
			IT-BCP（ITサービス継続計画）の策

Copyright © 2012 IPA, All Rights Reserved

項目	内容		
			定とマネジメント
			BCP とIT−BCP の関係
	②事業の重要業務と継続戦略	重要業務とそれに対するITサービス継続戦略の容や検討方法	事業のIT依存度
			重要業務
			重要業務選定の経緯と選定理由
			戦略検討の方法
			戦略の内容
	③重要業務のためのシステム基盤の概要	重要業務のシステム基盤の概要と構成の決定方法	構成
			選定理由と経緯
			技術的特徴
	④システム復旧対策のポイントと留意点	情報システム基盤の復旧対策にあたっての工夫点や震災時の効果、留意点	震災時の効果
			ポイント
			留意点や将来構想
	⑤高回復力システム基盤の要件と対策(要件内容)	高回復力システム基盤の要件と対策(要件内容)	高回復力システム基盤の要件と対策(要件内容)
調査時期	2012 年 4 月～5 月		

Copyright © 2012 IPA, All Rights Reserved

2. 事例編の活用と留意点

2.1. 事例編の活用の仕方

事例編は、実際に情報システム基盤の回復力を高めている組織の事例をもとに、高回復力システム基盤の導入や要件に関する情報をまとめたものである。

3 章で紹介する組織における対策事例に基づく参考となる情報や留意点は、以下の点で活用することができる。

・「高回復力システム基盤」導入の際の経緯や重要業務の考え方などを理解する。
・モデルシステムの選定や要件定義など導入手順のより具体的なポイントや方法を知る。
・モデルシステムごとにあらかじめ設定した要件内容と事例における対策(要件内容)との比較により、要件定義(特に要件調整)について具体的なポイントなどを知る。

4 章の「高回復力システム基盤構築におけるクラウドサービスの活用について」では、高回復力システム基盤の導入に活用できるクラウドサービス、並びにその効果および留意点を紹介しているので、各組織におけるクラウドサービス利用の検討において参照することができる。

2.2. 事例編の活用に際しての留意点

高回復力システム基盤導入計画の各手順(アクティビティ)と事例の記載項目の対応関係については、表 2.2-1 に示すとおりである。各作業手順を実施する際の参考として役立てて頂きたい。

表 2.2-1 事例と導入計画の関連

		高回復力システム基盤導入計画の手順(アクティビティ)			
		検討対象の選定	モデルシステムの選定	要件定義	導入計画策定
事例内容	(1)業種・組織概要	○			
	(2)検討対象の選定				
	①対象となるシステム基盤	○			
	②高回復力システム基盤構築の背景		○		
	(3)対象システムの概要		○	○	
	(4)要件定義			○	
	(5)導入にあたって				
	①構築にあたってのポイントや留意点				○
	②運用・見直しに関わる事項				○
	(6)対策例			○	○

高回復力システム基盤の要件については、各事例をモデルシステム１～4に分類し掲載しているが、事例の組織が実際にモデルシステムを選択した訳ではなく、「モデルシステムの主要な要件」に基づき、便宜的に分類したものであることに留意して頂きたい。

また、各モデルシステムにあらかじめ設定された要件内容と各事例の対策(要件内容)には、非機能要求レベルの差異が見られる。この差異を、各事例が持つ制約条件等を考慮して「モデルシステム選定」および

Copyright © 2012 IPA, All Rights Reserved

「要件定義」を行った結果であるとみなし、その背景、理由について推測、検討してみることは、実際に導入ガイドを用いて要件定義を実施する際の参考となろう。

さらに、各事例は、導入ガイドのモデルシステムの典型的な例として示しているのではなく、あくまでも一つの例としていることにも留意する必要がある。

Copyright © 2012 IPA, All Rights Reserved

3. 高回復力システム基盤の事例

2.2.事例編の活用に際しての留意点でも記載のとおり、事例編では 10 件の事例を対応するモデルシステムごとに分類して提示している。

3.1. モデルシステムと事例の対応づけ

「情報システム基盤の復旧に関する対策の調査報告書」のアンケート調査およびヒアリング調査対象のシステム基盤を、概要編で示す「モデルシステムの主要要件」に基づいて、モデルシステム 1～4 のいずれに該当するか分類した。

4 つのモデルシステムの特徴と主要要件は、表 3.1-1 のとおりである。

表 3.1-1 モデルシステムの特徴と主要要件

（概要編「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 か月	1～6 か月	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）

Copyright © 2012 IPA, All Rights Reserved

各モデルシステムに対応付けした 10 件の事例の概要は、表 3.1-2 に示すとおりである。

表 3.1-2 事例一覧

モデルシステム	事例ID	業種	重要業務	対策の特徴
1	1-1	製造業	・生産管理システム	・バックアップデータをメインサイトとは別の堅牢な建物の施錠キャビネット内に保管。
	1-2	サービス業	・基幹系のシステムは全て同じレベルで「重要」と位置付け ・情報システム部門としては、社員とのコミュニケーション基盤、次に受託開発業務	・遠隔地にオンラインバックアップを実施。
	1-3	地方公共団体	・住民基本台帳システム ・税務システム等	・東日本大震災で庁舎が津波により被災。遠隔地のバックアップデータで一部のデータを復旧。
2	2-1	サービス業	・Webサーバを使用した外部提供サービスとブロガーを管理するプライベート SNS	・データセンタと本社を活用した遠隔地データバックアップを実施。
	2-2	地方公共団体	・住民窓口サービス(各種申請・届出等手続き、証明書発行業務等)	・メインサイトは自設データセンタで冗長化、遠隔地バックアップを実施。
3	3-1	その他	・サービス利用者の契約者情報を管理するシステム	・阪神淡路大震災を契機に新規にシステムを構築し、同時に遠隔地にバックアップサイトを設置。
	3-2	サービス業	・ERPシステム(財務会計・人事管理・販売管理・ワークフロー)等で扱う基幹業務 ・メール・グループウェア等のコミュニケーション業務	・2箇所の民間データセンタを活用し、バックアップサイトを構築。クラウドサービスも活用。
4	4-1	サービス業	・最重要業務は、検査や認証等の管理業務である ・なお、構築しているシステム基盤には、経理関係等の社内向けのシステムを除き、ほとんどの業務システムが搭載されている	・サーバ仮想化技術採用し、バックアップサイトを設置。 ・同期バックアップを行い、震災時にフェイルオーバーを実施。
	4-2	金融・保険業	・金融商品取引業務	・システム障害対策のため、メインサイトは三重化を実施。
	4-3	製造業	・製造・販売・管理業務(対応システム:製造・販売・管理システム) ・顧客とのコミュニケーション(対応システム:メール等の情報系システム)	・水害によりサーバの水没の経験。 ・仮想化技術採用し、遠隔地サイトに同期バックアップを実施。

Copyright © 2012 IPA, All Rights Reserved

3.2. 事例の概要

3.2.1. 導入手順から見た各組織の取り組みの概要

本項では、事例全体を概観するための一助として、各事例のヒアリング調査内容を、表 2.2-1 に示した対応関係に基づき、計画編における導入手順(アクティビティ)ごとにまとめたものを示す。

アクティビティ2「モデルシステムの選定」およびアクティビティ3「要件定義」については、あわせて一項目としている。なお、事例が、各アクティビティの全ての事項についてカバーしているわけでないことにご留意いただきたい。また、各号のはじめにある枠囲みは、導入ガイド計画編に記載している各アクティビティの概要紹介である。

(1)アクティビティ1　検討対象の選定

計画編における＜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（システム基盤）」とする。検討対象が複数の場合の取組みの優先順位を定める。
- ・検討対象であるシステム基盤を選定するにあたって、経営層および事業部門の視点から最初に重要業務を識別し、次に当該重要業務に関連するアプリケーションを特定し、最後にアプリケーションの稼働に必要なシステム基盤を選定するというアプローチを採用している。
- ・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。
- ・担当者は、組織の特性や制約に応じて、適当なアプローチを検討・採用することが望ましい。

①事例における重要業務の定義や考え方について、参考となる点としては以下の事項が挙げられる。

- ・事業レベルで BCM(事業継続マネジメント)が導入されている場合は、その取り組みの中で決定されている。
- ・主要な事業や収益の源泉となる業務を重要業務としている事例が多くあった。
- ・法令上規定されている業務や、顧客と SLA を締結している場合、その内容を重要業務としている。
- ・災害発生後の対策(救助、救援、安否確認など)も重要業務としている。
  （地方公共団体等はもちろんのことだが、災害等の経験から企業等にも同様の事例があった。）
- ・非常時での必要性が必ずしも高くない業績把握や情報提供を行うシステムの優先順位は、比較的低いとしている。

②留意点としては、以下の事項が挙げられる。

- ・情報システム部門で独自に重要業務を決定し、その結果について社内で承認されてないと思われる事例があった。重要業務の識別については、経営陣をはじめとした関係部門との確認や合意を取ることが必要である。

Copyright © 2012 IPA, All Rights Reserved

⑵アクティビティ 2　モデルシステムの選定とアクティビティ 3　要件定義

計画編における＜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、検討対象となる業務の障害時・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。

計画編における＜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。

①「モデルシステムの選定」と「要件定義」について、参考となる点としては以下の事項が挙げられる。
・情報システムの高回復力に関わる要件の見直しは、被災や障害等や、経営層の指示、監査の指摘等を契機に行われている。また、システム基盤の性能向上やコスト低減、運用改善等の一環として高回復力に関わる要件の見直しが行われている事例もあった。
・事例にみる投資・費用の決定過程の概要は以下のようであった。
－情報システム部門が数社の業者から情報収集を行い、要件や対策の検討などを行っている。
－経営層や全社のIT運営委員会などのIT投資に関する意思決定機関などによって、審議や決定が行われる。
－その決定に基づき、情報システム部門が導入を進める。
・IT関連費用について、費用規模の枠を対売上高などの割合で定めている事例もあった。

②留意点としては、以下の事項が挙げられる。
・システム障害、とりわけハード故障についての復旧目標はほとんどの事例で設定されていたが、大規模災害時のシステム再開目標を具体的に定めていたのは 3 事例であった。通信や電力供給などの外部サービスも含め、システム基盤の構成要素が、災害により機能しなくなることを前提に復旧目標を定めることが望まれる。
・情報システムの高回復力にかかわる要件の見直しについては、問題発生後に行われているケースもあったが IT サービス継続のためのマネジメントシステム（PDCA サイクル）を整備し、運用し、認識されたリスクに応じて事前に対処することが望ましい。
・モデルシステム選定や要件定義を実施する際に確認したり検討したりする目標復旧時間、システム規模、要件等については、各事例の以下の項目などが参考となる。
－対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)
－高回復力システム基盤の概要(システム構成等)
・各モデルシステムにあらかじめ設定された要件内容と、事例の要件内容の差異の理由は、今回のヒアリングでは十分な確認をしていない。検討対象の要件内容は、あらかじめ設定した要件内容に基づき必要とするRTO やその他の要件等によって調整可能であるとともに、各組織における可能な投資額によっても調整する必要がある。

Copyright © 2012 IPA, All Rights Reserved

(3)アクティビティ4　導入計画策定

計画編における＜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る。
・導入計画策定や実際の導入にあたっては、各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、それに準拠し、ない場合は共通フレーム 2007 等の標準に準拠して進めることが望ましい。

①「導入計画策定」(特に「対策の定義」)について、参考となる点としては以下の事項が挙げられる。

・高回復力システム基盤導入のための技術やサービスの選定・構築について、目標を達成しつつ運用上コスト等の負担を適切なものとするために、有効性や制約等を十分検討・検証している事例が多くみられた。
　－デスクトップの仮想化によりクライアント端末の復旧スピードが向上した事例では、最適なサーバを選択するために 50 台のデスクトップ環境を動作させ、サーバのサイジングの検証を繰り返した。
　－モデルシステム 4 に相当する事例では、ビジネスの競争力を高めるため、要求性能が高いにもかかわらず市販品でハードウェア等を構成しコストを低減した。
　－仮想化によるシステムの統合作業とバックアップサイトの設置を同時に進めることにより、サーバ台数を削減しシステム運用の効率性を高めるとともに、ITサービスの継続性を確保した。
　－ERPシステムを任せている委託先事業者と、それ以外のシステムを任せている委託先事業者の 2 社にフルアウトソーシングしている。これにより、データセンタ利用料等の委託先事業者に支払うコストは以前より増加したが、社員の負担は大幅に軽減された。
・バックアップについては、バックアップデータを取得するのみならず、リストアやバックアップの保管に関するルールや手順の策定などの取り組みがみられた。また、バックアップやフェイルバック(バックアップサイトへ切り替えた後、再度、本来のメインサイトへ戻すこと)について、以下のような参考となる事例があった。
　－バックアップサイトへの切り替えは、経営判断(緊急時対応の発令等と思われる)により行うため、手動により切り替えを行う手順にしている。(この例とは別に、自動的に切り替える仕組みにしている事例もあった。)
　－フェイルバックには 2 週間ほど要した。データを最新化するのに時間を要したためである。当時フェイルバックの経験や標準手順が確立していなかったが、現在は手順が確立したので、1 週間程度で実施可能である。
　－情報セキュリティの観点から、バックアップデータは暗号化して保管している。
・震災の混乱期においても円滑に業務を継続できたのは、大規模地震が発生した場合の業務への影響を分析し、事業継続を行うための対策や対応手順を策定していたからだと考えられる。また、定期的に実施している演習や教育訓練も効果を発揮した。
・それぞれの事例の最後に、高回復力システム基盤の要件に対応する対策例を、「高回復力システム基盤の要件と対策(要件内容)」として掲載している。

Copyright © 2012 IPA, All Rights Reserved

②留意点としては、以下の事項が挙げられる。

・導入ガイドでは、業務データ等のバックアップについては、特にバックアップを取得することを中心に紹介しているが、バックアップデータをリストアして業務復旧することや、バックアップサイトに切り替えて業務再開したのちメインサイトに戻す場合の取り組み(フェイルバック)についてもあらかじめ検討しておくことが望まれる。

・紹介している事例では、「将来構想」として改善や追加の対策を行うと回答しているものもある。これらの改善や追加対策の中には、高回復力システム基盤を導入しようとする際に参考とすべきものが含まれている。

高回復力システム基盤の構成要素についての改善や追加の対策にする事項は、表 3.2.1-1 のとおりである。

表 3.2.1-1 高回復力システム基盤の構成要素についての改善や追加の対策

高回復力システム基盤の構成要素	改善や追加の対策
業務データ・業務アプリケーション(ソフトウェア)	遠隔地バックアップ。さらにリアルタイムバックアップ
情報処理施設の代替	バックアップサイトの所在地の見直し クラウドの利用
システム運用の体制や仕組み	復旧の手順書の充実
ハードウェア機器やネットワーク機器や通信・電力等のサービス	システムの重要度と停止許容時間をもとにした冗長化の必要性の検討 通信等のサービスが停止したときの事業継続方法の検討

Copyright © 2012 IPA, All Rights Reserved

3.2.2. 要件から見た各組織の取り組みの概要

本項では、事例全体を概観するための一助として、各事例の内容のうち特に対策(要件内容)について、計画編で示した高回復力要件の分類(前提要件、主要要件[1]、考慮要件)ごとにまとめたものを示す。

また、各モデルシステムにあらかじめ設定した要件内容と、各事例における対策(要件内容)が比較できる一覧を、付録「高回復力システム基盤の要件と各事例との対比表」に示す。

(1)前提要件に関する事例の対策(要件内容)

計画編では、前提要件はモデルシステムごとにあらかじめ設定された要件内容を持たない。要件定義の最初の段階における前提要件を設定する際に、各事例の対策(要件内容)を参考にするとよい。

各事例における、前提要件に対応する対策(要件内容)については、次に示す傾向がある。

・システム障害、とりわけハード故障についての復旧目標はほとんどの事例で設定されている。

・RLO(目標復旧レベル)については、事例ではそれぞれの必要とするレベルやコストを含めた制約等のため、ばらつきが大きい。

・また、大規模災害時のシステム再開目標について具体的に定めている事例は多くなかった。

(2)主要要件に関する事例の対策(要件内容)

計画編では、主要要件について、モデルシステムごとの要件内容をあらかじめ設定している。

各事例の対策(要件内容)と、モデルシステムごとにあらかじめ設定された要件内容を比較し、その際について考察してみることは、モデルシステムを選定した後、要件調整を行う際の参考となる。

各事例における、主要要件に対応する対策(要件内容)と、モデルシステムごとにあらかじめ設定された要件内容を対比すると、次に示す傾向がある。

・モデル 4 の事例を除き、あらかじめ設定した要件内容を上まわるネットワーク機器・ネットワーク・ストレージの冗長化構成をとっているシステムはない。(ネットワーク機器は冗長化でなく予備機で高回復力を実現していると思われる。)

・一方、運用監視については、あらかじめ設定した要件内容を上まわる種類の情報を監視している事例が多い。

・定期保守は実施していない事例が多い。その理由として、以下のようなことが挙げられている。

－故障の予兆情報を監視しているため必要を感じていない。

－24時間365日停止できないシステムであるため定期保守は実施しない。

－定期保守することにより、トラブルが発生することを恐れている。

－通常の保守メニューにないため導入時にベンダから提案がなかった。等

[1] 表 3.1-1 中の「モデルシステムの特徴」および「モデルシステムの主要要件」にも、同名の要件が存在するが、これらはモデルシステム選定の目安となるよう、暫定的で大まかな要件内容が設定されているものである。

Copyright © 2012 IPA, All Rights Reserved

(3)考慮要件に関する事例の対策(要件内容)

計画編では、考慮要件はモデルシステムごとにあらかじめ設定された要件内容を持たない。考慮要件を設定する際に、各事例の対策(要件内容)を参考にするとよい。

各事例における、考慮要件に関する事例の対策(要件内容)については、次に示す傾向がある。

・ベンダ側対応者の要求スキルレベルについて、回答の中では明文化して要求しているところは少ないが期待レベルは持っている。一方、実際に対応している対応者のスキルレベルについては、把握していて、満足していることが多い。
・定期報告については、障害報告はあげられるようになっているが、会議体として定期的に実施しているは、半数の組織であり、多くの場合月次で行っている。

Copyright © 2012 IPA, All Rights Reserved

3.3. 各モデルシステムの事例

10 件の個別事例を、モデルシステムごとに分類して紹介する。
なお、事例の記述内容はヒアリング調査結果を掲載したものであり、各項目の表題と内容が必ずしも整合しないように見える個所もあるが、当該項目に対するヒアリング先の回答内容がそのまま伝わることを重視し、余り編集を加えていないことによるものとご理解いただきたい。

Copyright © 2012 IPA, All Rights Reserved

3.3.1. モデルシステム 1 の事例

(1)事例 1-1

業種・組織概要		
業種		製造業
業務内容		機械製造業
従業員数		約 300 名
検討対象の選定		
対象となるシステム基盤	重要業務	生産管理システム
	業務選定の理由	最も重要なのは、日々の製造作業を管理する生産管理システムであり、全社的な共通認識である。経理システムの支払い処理も重要であるが、処理が集中するのは月末であるため、優先順位は比較的低い。
高回復力システム基盤構築の背景	経緯	バックアップ媒体をサーバ設置場所とは別なビル内の施錠キャビネットに保存するようにしたのは、監査における公認会計士の指摘による。
	投資額の決定、経営者の関与等	社内にはIT運営委員会が設置されており、IT投資に関する企画等については委員会で審議される。承認を得た企画は、情報システム部門で具体的化し、導入・運用・保守に関する外部委託先との契約を実施する。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・目標復旧時間(RTO)は、故障発生時半日程度である。 ・大規模災害時は、2 週間を復旧目標としている。サーバのメーカーから代替機の用意に 2 週間かかるという情報を得ており、これが遅れなければ実現可能な目標値と考えている。具体的にシミュレーションした期間ではない。 ・目標復旧レベル(RLO)について、対象システムは生産管理、財務、経理システムの 3 つ全てである。復旧レベルはシステムのレスポンスが平常時より低下することは許容するレベルである。代替機として、平常時と同じサーバ構成が取れないケースも想定している。 ・目標復旧時点(RPO)は、障害発生前日のバックアップ時点まで復旧する。
高回復力システム基盤の概要	規模	・メインサイト：サーバ 4 台 ・クライアント端末数：150 台 ・東京に本社および工場、大阪に営業所あり。
	システム構成と復旧対策の概要	・メインサイトのサーバは非冗長化構成。 ・バックアップは 1 日 1 回、フルバックアップを実施。 ・バックアップ媒体はサーバ設置場所とは別なビルの施錠キャビネット内に 3 週間分保存。 ・システム構成の概要を図 3.3.1-1 に示す。
導入にあたって		
構築にあたってのポイントや留意点		サーバは冗長化構成とはしていないが、故障時には保守委託先事業者が数時間以内に駆け付け修理するので、システム停止時間は半日程度にとどまり業務に大きな影響を与えたことはない。
運用・見直しに関わる事項	震災時等の効果	直接の影響は無かった。大地震が起きた際には、どこにどのような連絡をして、どのような対応をするなど現状で何ができるかといった観点からの、災害時の対応フローを作成した。
	将来構想	・バックアップデータをリストアしてシステムが正常動作することを確認していない。今後は実施したい。 ・東京にしかデータが無いのは不安であり、外部へのデータを保管は検討したい。ただ、小規模企業では単独でシステムを検討するのは困難であり、小規模企業向けのバックアップに関するガイドラインのようなものがあれば利用したい。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.1-1 のとおり。		

Copyright © 2012 IPA, All Rights Reserved

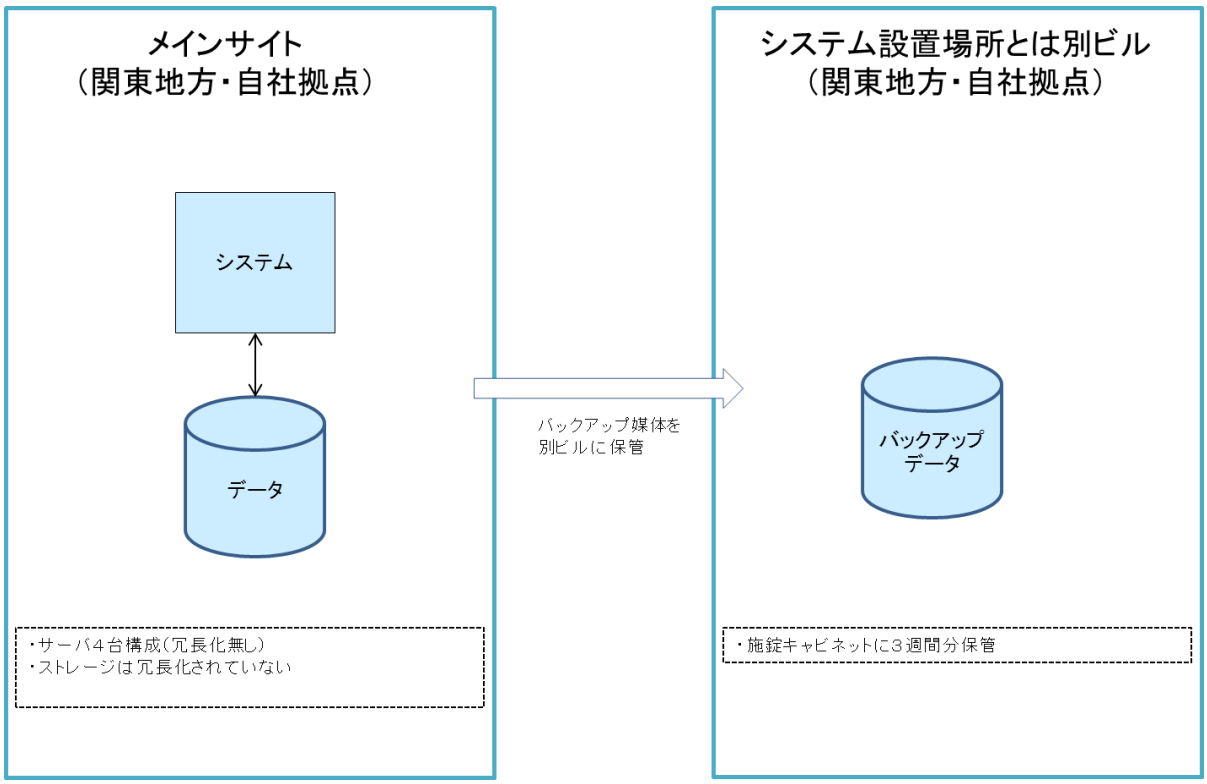

図 3.3.1-1 システム構成の概要

表 3.3.1-1 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	業務停止を許容している。
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	日次バックアップからの復旧
	A.1.3.2				RTO(目標復旧時間)	半日程度
	A.1.3.3				RLO(目標復旧レベル)	全ての業務
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	2 週間
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	非冗長化
	A.2.1.2				冗長化(コンポーネント)	非冗長化
	A.2.3.1			ネットワーク機器	冗長化(機器)	非冗長化
	A.2.3.2				冗長化(コンポーネント)	非冗長化
	A.2.4.1			ネットワーク	回線の冗長化	非冗長化
	A.2.4.2				経路の冗長化	非冗長化
	A.2.5.1			ストレージ	冗長化(機器)	重要システムにストレージは導入していない

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
	A.2.5.2				冗長化(コンポーネント)	重要システムにストレージは導入していない
	A.2.5.3				冗長化(ディスク)	内蔵ハードディスクについて RAID5
	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
	A.2.6.3				データインテグリティ	非回答
	A.3.1.1		災害対策	システム	復旧方針	代替機による同等の構成
	A.3.2.1			外部保管データ	保管場所分散度	サーバ設置場所とは別の堅牢なビルに設置した施錠キャビネットに保管している
	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	死活監視とエラー監視を実施している
	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	定期保守を実施しない
	C.2.6.1			予防保守レベル	予防保守レベル	予防保守を実施しない
	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	復旧は保守委託先が手作業で実施する
	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	数時間内
	C.3.3.3				SE到着平均時間	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	交換部品について年数の延長などは要求してない
	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	ユーザマニュアルはシステム管理部門で作成する(故障対応手順等は委託先事業者が実施するため、未作成である)
	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	建築は 2 年前なので震度 6 強に耐えられる
	F.4.4.4			電気設備適合性	停電対策	UPSにより、10分程度の電源確保することができる
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	全て委託先事業者にて実施している
	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	明文化していないが、修理方法を特に指示しなくとも実施できるレベルである
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	従業員は、システム操作研修に参加しているが、復旧作業の研修は実施していない
	C.5.9.1			定期報告会	定期報告会実施頻度	実施していない
	C.5.9.2				報告内容のレベル	障害報告のみ

Copyright © 2012 IPA, All Rights Reserved

(2)事例 1-2

業種・組織概要		
業種		サービス業
業務内容		おもな事業内容は、エンジニアコンサルティング、システム開発、パッケージ販売。昨今では受託によるシステム開発事業の比重が高い。
従業員数		約 600 名
検討対象の選定		
対象となるシステム基盤	重要業務	・重要業務は、現 BCP では明確に定めていない。 ・結果的に、現状は基幹系のシステムは全て同じレベルで「重要」と位置付けられており、全てバックアップを行ってきた。これまでは、システム障害が発生する規模の災害は起こらなかったため、復旧の優先順位をつけるといった場面は発生しなかった。 ・情報システム部門としては、社員とのコミュニケーション基盤の復旧が最重要だと考えている。次に受託開発業務であり、開発中のソフトウェアを守る必要がある。
	業務選定の理由	・当社の商品・サービスは社員の知識・ノウハウを形にして売る業種であることから考えると、被災時に顧客対応を早急に行うためには、社員とのコミュニケーション基盤の早期復旧が最重要だと考えている。また、開発中の顧客のシステムが保全されていないと事業が成り立たない。ただし、これは全社的な考えではなく情報システム部門としての考えである。
高回復力システム基盤構築の背景	経緯	・遠隔地でのバックアップは、3 年前の BCP 策定時から行っている。バックアップは対策の中でも取り組みやすい部分であることから、ここから取り組み始めた。災害対策という観点だけでなく、開発中システムの障害対策としてもバックアップが必要であった。
	投資額の決定、経営者の関与等	・情報システム部門が 3 業者から情報収集を行い、バックアップ方法や機器を選定。経営層の決裁を得て実施した。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・ビジネスインパクト分析(BIA)を行っておらず、全社的な検討は行っていない。 ・情報システム部門としては、最優先に復旧すべきコミュニケーション基盤については、およそ以下の復旧が求められると考えている。 [目標復旧時間(RTO)] ・10～30 分 [目標復旧レベル(RLO)] ・障害・被災前より業務・機能を制限したレベル [目標復旧時点(RPO)] ・障害・被災発生の直前まで復旧
高回復力システム基盤の概要	規模	・システムとしては、1)社内用システム(財務会計管理、人事、メール・グループウェア等多数)、2)受託によって開発した顧客用システムに分けられる。 ・メインサイトサーバは 100 台以上に上っており、②の顧客用システムに利用しているファイルサーバやテスト用サーバが半分程度を占めている。
	システム構成と復旧対策の概要	・各システムのサーバは東京都内の 2 か所の社屋ビルに設置しており、バックアップサイトを熊本の事業所においている。 ・データバックアップは、上記に示した 1)、2)共に行っている。メインサイト内でのバックアップに加え、更に遠隔地のバックアップサイトにてバックアップを行っている。ハードディスクでのバックアップであり、データ容量としては 2)のファイルサーバ分が大きい。メインサイト内でのバックアップ、遠隔地でのバックアップ共に、バックアップ頻度は週 1 回である。容量が大きい(100 テラバイト以上)ため、毎日分散してバックアップを実施しており、個々のデータのバックアップ頻度は週 1 回となる。理想的には、毎日実施したい。 ・いったんメインサイト内でバックアップしたものを、遠隔地へ移している。メインサイト内、遠隔地でのバックアップ共に、システムによって実施曜日が異なる。遠隔地へのバックアップは 100Mb/s のインターネット VPN 回線を利用したオンラインバックアップである。 ・なお、財務会計管理システムは遠隔地に待機系システムがある。これは遠隔地に同システムの開発環境があり、これを待機系として活用することができるからである。財務会計管理システム以外のシステムについても待機系システムを置くことが理想だが、予算面で実現できていない。 ・システム構成の概要を図 3.3.1-2 に示す。

Copyright © 2012 IPA, All Rights Reserved

導入にあたって		
構築にあたってのポイントや留意点		・日常的に利用していないシステムは、緊急時にすぐに操作できるかといった問題がある。安否確認システムなど、緊急時に初めて使うものでなく、日常的に利用するシステムの機能の一つとして構築することが理想である。
運用・見直しに関わる事項	震災時等の効果	・東日本大震災の際、サーバに障害が発生したため、バックアップデータにより復旧できた。今後は、データの重要性見直しや不要データ整理が必要だと考えている。
	将来構想	・現在は社内用システム、顧客用システムの管理や保全の方針が混在しているが、今後はそれぞれを区別して方針を定め、どのようにしてシステム保全を図るべきか整理しなければならない。 バックアップの保管基準を定めたいが、顧客によっては、古いバージョンのシステムも保管を求められるため、バックアップデータの整理においては、留意が必要となっている。 ・クラウドについては、遠隔バックアップ費用の軽減の点から興味を持っている。遠隔バックアップ用のサーバ機器は高価であり、クラウドであれば軽減が期待できる。ただし、クラウドのセキュリティに対する不安があり導入に踏み切れない。また、顧客によっては外部へのデータ持ち出しを禁止する場合もある。クラウドのセキュリティ評価基準などがあれば、顧客に対しても説明しやすいが、現状では難しい。 社員の安否確認システムなどでのクラウド利用は考えられる。現在利用しているシステムは、メールでの確認を基本としており、東日本大震災ではメールの利用制限がかけられたため使うことができなかった。メールよりも制限が弱いWebベースのシステムをクラウドで構築することは有効かと思われる。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.1-2 のとおり。		

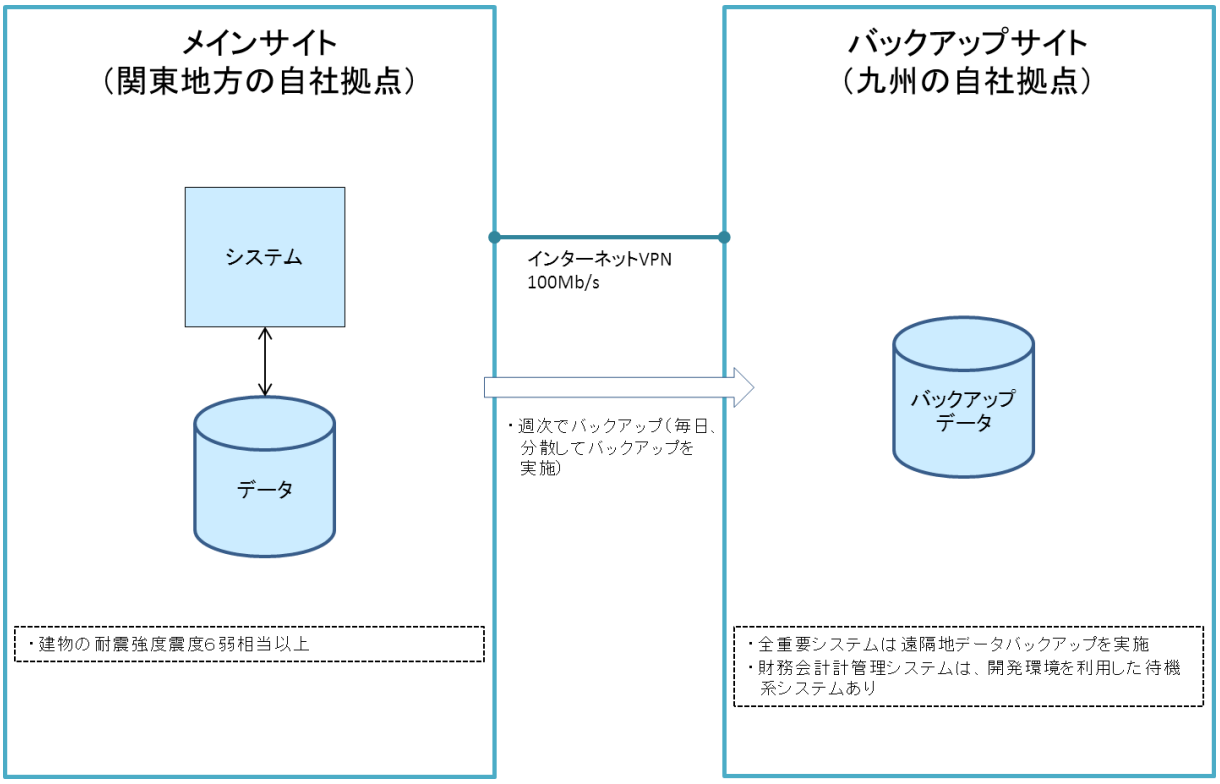

図 3.3.1-2 システム構成の概要

Copyright © 2012 IPA, All Rights Reserved

表 3.3.1-2 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	メインサイト・遠隔地のバックアップサイト双方が利用できない際には、システムは利用できない
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	未設定。障害・被災発生の直前まで復旧したい。
	A.1.3.2				RTO(目標復旧時間)	未設定。10～30 分未満を目指したい。
	A.1.3.3				RLO(目標復旧レベル)0	未設定。障害・被災前より業務・機能を制限した水準を目指したい。
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	1 週間程度と考えられる。
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	一部冗長化している
	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)	非冗長化
	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	非冗長化
	A.2.4.2				経路の冗長化	非冗長化
	A.2.5.1			ストレージ	冗長化(機器)	特定の機器のみ冗長化している
	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を行っている。
	A.2.6.3				データインテグリティ	データの完全性を保証(エラー検出＆訂正)
	A.3.1.1		災害対策	システム	復旧方針	未対策
	A.3.2.1			外部保管データ	保管場所分散度	1 か所(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	メールシステムはパフォーマンス監視を実施
	C.1.3.2				監視間隔	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	定期保守を実施しない
	C.2.6.1			予防保守レベル	予防保守レベル	予防保守を実施しない
	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	復旧作業は全て手動
	C.3.3.1			システム異常検知時の対応	対応可能時間	ベンダの営業時間対応(9～17 時)
	C.3.3.2				駆けつけ到着時間	センドバック保守。電話対応は随時。
	C.3.3.3				SE到着平均時間	財務会計は一部自社開発。他社開発部分については翌営業日。
	C.3.4.1			交換用部材の確保	保守部品確保レベル	保守契約に基づく規定年数の確保。
	C.3.4.2				予備機の有無	ネットワーク機器については予備機あり
	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する

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
	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	新館の耐震強度は震度 6 強、本館は震度 5 弱である。
	F.4.4.4			電気設備適合性	停電対策	UPSにより1時間程度の電源を確保することができる。
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	一部ユーザが実施している。
	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	受託当時のシステム開発者が対応しており、ユーザの事情にも通じている。
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	実施していない。
	C.5.9.1			定期報告会	定期報告会実施頻度	行っていない。
	C.5.9.2				報告内容のレベル	なし

Copyright © 2012 IPA, All Rights Reserved

(1)事例 1-3

業種・組織概要		
業種		地方公共団体(東日本大震災被災自治体)
業務内容		行政サービス等の地方自治業務
従業員数		300 名弱
検討対象の選定		
対象となるシステム基盤	重要業務	・住民基本台帳システム ・税務システム等
	業務選定の理由	・被災した際のシステム復旧における優先順位である。震災直後の混乱期であったため上層部とは、大枠の打ち合わせを行い、詳細は、総務課職員と担当課職員で判断した。 ・住民や事業者に関わる業務の復旧優先順位が高いと判断した。特に、住民の安否確認、り災証明発行を行う窓口業務、復旧資金の出し入れを行う会計業務の緊急性が高かった。
高回復力システム基盤構築の背景	経緯	・情報システム用に確保できる電源容量や空調設備なども明確になっていなかったため、できるだけ省スペース・省電力となる構成を検討した。 ・震災前には、DAT テープによるデータバックアップを行っていたが、媒体の交換や管理等で職員の作業負担が大きかったため、ストレージ内にバックアップを保管する方式に変更した。なお、震災による津波でサーバ設置場所に保管していたテープは使用できなくなっており、データの復旧には役立たなかった。 ・ハードウェア環境の変更以外は、震災前の状態への復旧を再優先としたため、データセンタやクラウドの利用は検討しなかった。(通信回線の断絶が長期に及んだので、利用したくともしばらく利用できなかったと思われる。)
	投資額の決定、経営者の関与等	・震災直後の混乱期であったため、上層部とは大枠の方針について合意した上で、復旧を進めた。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・目標復旧時間(RTO)は未設定。ハードウェア故障程度であれば、限りなくゼロに近いことが理想である。 ・目標復旧レベル(RLO)は未設定。システムの復旧優先順位としては設定している。 ・目標復旧時点(RPO)は未設定。一部システムでは、リアルタイムでのバックアップを実施している。障害発生直前までデータリカバリできるのが理想である。
高回復力システム基盤の概要	規模	・サーバ数:計 30～40 台(ブレードサーバ) ・クライアント端末数:300 台 ・ストレージを数台利用し、サーバとストレージは SAN により接続している。
	システム構成と復旧対策の概要	・一部サーバは負荷分散を目的とした 2 台構成としており、1 台のみの故障時は業務継続が可能である。但し、手動による切り替えが必要となる。 ・月に 1 回データの一部を媒体により、委託先事業者に送付している。 ・メインのバックアップはストレージ内に保管している。 ・システム構成の概要を図 3.3.1-3 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・サーバをブレードサーバとすることで、省スペース・省電力を実現した。 ・DAT の使用をやめ、ストレージをバックアップの保管先とすることにより、DAT の交換・管理に関する職員の負担を軽減することができた。 ・委託先事業者が遠隔システム監視を実施しており、エラー監視・リソース監視も実施している。異常を発見すると、委託先事業者が遠隔ログインしタイムリーに調査してくれる。委託先事業者の駆け付けに時間がかかる土地であるが、これを補っている。
運用・見直しに関わる事項	震災時等の効果	・現在のシステムは震災後に構築したものだが、震災前のデータバックアップ対策では不十分であった。バックアップ用の DAT は全て破損し復旧の役には立たなかった。被災したハードディスクをサルベージしたり、あるいは委託先事業者に預けたデータを利用したりする等して復旧した。それでも、全ては復旧できず手作業で復旧しているものもある。
	将来構想	・現在、サーバを設置している仮庁舎は高台にあり津波の心配は無いが火災等は可能性があるため、バックアップの遠隔地保管は必要と考えている。コストに見合えば、ネットワーク経由

Copyright © 2012 IPA, All Rights Reserved

		でリアルタイムにバックアップするのが理想である。 ・業務特性によって、リアルタイムでのバックアップが必要なシステムと、前日のバックアップでも対応できるシステムがある。各システムのバックアップの重要性を整理した上で、バックアップ方式や頻度等を整理しておくべきである。ただし、職員だけで各システムのデータ保全のレベルを優先順位づけすることは非常に困難であり、目安になるものがあればよいと思う。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.1-3 のとおり。		

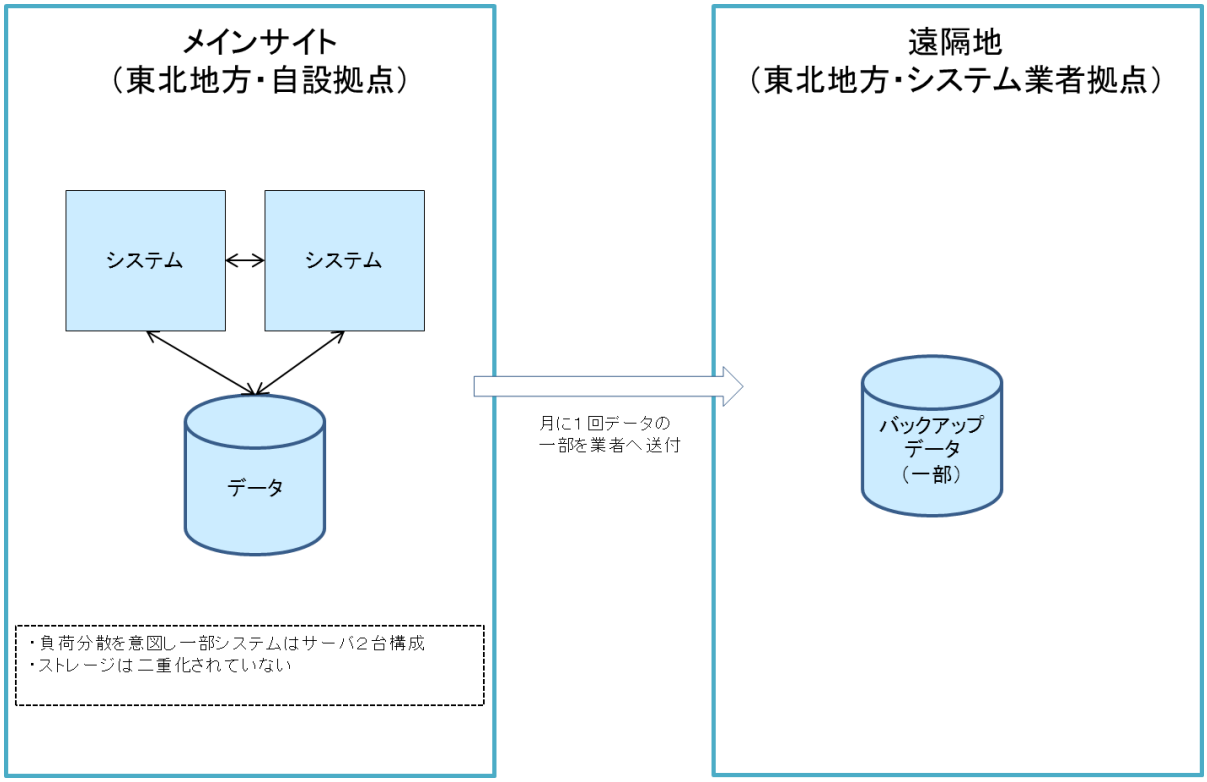

図 3.3.1-3 システム構成の概要

表 3.3.1-3 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	一部サーバは冗長化されており、単一障害でも業務継続できる
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	障害発生時点(一部システム)
	A.1.3.2				RTO(目標復旧時間)	数値としては定めていない
	A.1.3.3				RLO(目標復旧レベル)	窓口業務が最も優先順位は高いが、全業務が復旧対象となる
	A.1.4.1			目標復旧水準(大規模	システム再開目標	数値としては定めていない

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
				災害時)		
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	一部冗長化している
	A.2.1.2				冗長化(コンポーネント)	エンクロージャーの電源、FAN などを二重化している
	A.2.3.1			ネットワーク機器	冗長化(機器)	ルータ・コアスイッチは部分的に二重化している。フロアスイッチ(L2)や HUB などの一部は予備機を保有している
	A.2.3.2				冗長化(コンポーネント)	ルータ・コアスイッチの電源・FAN は二重化している
	A.2.4.1			ネットワーク	回線の冗長化	非冗長化
	A.2.4.2				経路の冗長化	一部経路のみ冗長化されている。
	A.2.5.1			ストレージ	冗長化(機器)	非冗長化
	A.2.5.2				冗長化(コンポーネント)	電源・FAN 等の二重化できる部分は二重化している。
	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
	A.2.6.3				データインテグリティ	一部システムでエラー検出を実施。その他は不明。
	A.3.1.1		災害対策	システム	復旧方針	仮庁舎は、高台にあるので津波の心配は不要だが、火災等を考えると対応が必要。
	A.3.2.1			外部保管データ	保管場所分散度	一部データを月 1 回委託先事業者に預けている。
	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	死活監視に加え、サーバのハードウェア的なエラー情報、リソース使用量などを監視している。
	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	定期保守は実施しない(エラー監視はシステムで実施しており不要)
	C.2.6.1			予防保守レベル	予防保守レベル	監視システムにより、故障の予兆状況を検出
	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	復旧自動化は行っておらず、障害時は遠隔操作により復旧対応している
	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	数時間内
	C.3.3.3				SE到着平均時間	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	保守契約に基づく規定年数の確保
	C.3.4.2				予備機の有無	一部のネットワーク機器のみ予備機を保有している。
	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	委託先事業者が保有する一般的なマニュアルを利用している(業務システムについては存在したが消失した)
	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	現在、プレハブ造りの仮庁舎であり、耐震性能は不明。
	F.4.4.4			電気設備適合性	停電対策	自家発電装置により、数時間電源を確保することができる

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	遠隔ログイン環境で、全て委託先事業者が実施する。現地でしかできない作業は、職員が協力することもある
	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	契約では定めておらず、要求仕様にも示してはいないが、導入したシステムのハードウェア・ソフトウェアの全てに対応できるレベルが求められる。これまでに同システムを導入した実績を有する対応者が対応している
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	必要性は感じているが、現時点では訓練を行っていない
	C.5.9.1			定期報告会	定期報告会実施頻度	実施していない
	C.5.9.2				報告内容のレベル	障害報告のみ

Copyright © 2012 IPA, All Rights Reserved

3.3.2. モデルシステム 2 の事例

(1)事例 2-1

業種・組織概要		
業種		サービス業
業務内容		主としてインターネットサービス(Web等)を主軸とした商品プロモーション業務
従業員数		10 名
検討対象の選定		
対象となるシステム基盤	重要業務	・Webサーバを使用した外部提供サービスとブロガーを管理するプライベート SNS
	業務選定の理由	・サービスが停止すると業務に与える影響が最も大きいことから、重要業務とした
高回復力システム基盤構築の背景	経緯	・信頼性対策について実施すべきことは実施する方針と、コストとの兼ね合いから現在の構成としている。 ・以前は、安定性とパフォーマンスを確保するため、サービスごとに専用サーバを設置し、ロードバランサーを使用して 1 サービスあたり数台のサーバ構成としていたが、オーバースペックであることが判明し、サーバ性能が向上したこともあり、サーバ統合を行い現状の構成とした。サーバ仮想化に関しては情報収集中といったところである。
	投資額の決定、経営者の関与等	・技術担当役員と社長とで相談して決めている。 ・IT関連費用は売上高の 10%程度になる。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・目標復旧時間(RTO)は、ハード故障時 24 時間としている。コールドスタンバイしたサーバの予備機に環境を作成し、バックアップデータのリストアを実行して復旧するまでに、必要な時間を想定している。 ・目標復旧レベル(RLO)は、故障発生前と同等の状態へ復旧する。 ・目標復旧時点(RPO)は、前日のバックアップ取得時まで復旧する。
高回復力システム基盤の概要	規模	・メインサイト:10 台程度。(商用データセンタに設置) ・利用者数:同時利用者数はサーバ 1 台当たり 100 名程度。サーバ利用状況は最も多いサーバで 500 万 PV/日。
	システム構成と復旧対策の概要	・メインサイト(商用データセンタ)のサーバは 1 日 1 回フルバックアップを実施している。 ・メインサイトのバックアップデータはネットワーク経由で転送し、自社拠点サーバのハードディスクに保存する。 ・メインサイト内にコールドスタンバイしたサーバを準備しており、ハードウェア故障時に使用する。 ・システム構成の概要を図 3.3.2-1 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・システムに関しては費用削減を重視している。 ・オフィスからの遠隔によるサービス監視、データバックアップのソフトウェアは自社開発した。高価なソフトウェアを購入しなくとも、自社で開発した方が費用をかけずに済むケースもある。 ・サービスに利用する機器は、多数の製品の口コミ情報を集め故障の少ないメーカ・ブランドから選定を行っている。ハードディスク以外の部品は故障率が低いことが経験上わかっているので、ハードディスク以外の部品は冗長化していない。 ・サーバは、機器をエージング (納品事前に電源を投入し動作確認)させて納品してくれる販売業者から購入しているので、初期不良も少ない。 ・ハードウェアの定額保守契約は締結していない。故障の場合、予備機を利用して復旧し、センドバックで修理を依頼する。
運用・見直しに関わる事項	震災時等の効果	・直接の影響は無かった。また、システムの対策見直しには至らなかった。
	将来構想	・復旧の手順書については、さらに充実してゆきたい。
対策例		

Copyright © 2012 IPA, All Rights Reserved

高回復力システム基盤の要件と対策(要件内容)は表 3.3.2-1 のとおり。

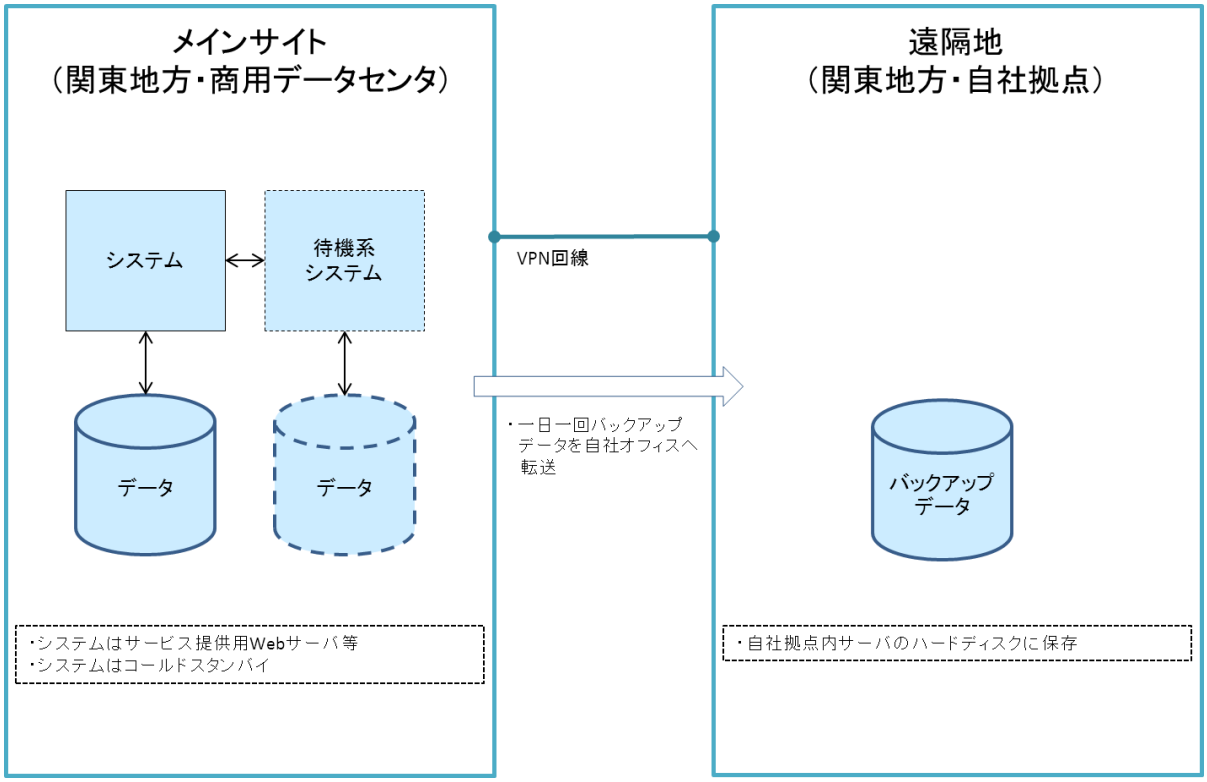

図 3.3.2-1 システム構成の概要

表 3.3.2-1 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	障害時の停止を許容する
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	日次バックアップからの復旧
	A.1.3.2				RTO(目標復旧時間)	24 時間以内
	A.1.3.3				RLO(目標復旧レベル)	障害発生前と同等のレベル
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	24 時間未満(データセンタが無事の前提)
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	コールドスタンバイ
	A.2.1.2				冗長化(コンポーネント)	非冗長化
	A.2.3.1			ネットワーク機器	冗長化(機器)	非冗長化
	A.2.3.2				冗長化(コンポー	非冗長化

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
					ネント)	
	A.2.4.1			ネットワーク	回線の冗長化	非冗長化
	A.2.4.2				経路の冗長化	非冗長化
	A.2.5.1			ストレージ	冗長化(機器)	非冗長化
	A.2.5.2				冗長化(コンポーネント)	非冗長化
	A.2.5.3				冗長化(ディスク)	RAID1 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
	A.2.6.3				データインテグリティ	エラー検出なし
	A.3.1.1		災害対策	システム	復旧方針	データセンタ被災時の対策は、最低限のサービスを選定し、Bフレッツ回線に振り向けて提供できるようにすることを検討している
	A.3.2.1			外部保管データ	保管場所分散度	データセンタと社内に保管
	A.3.2.2				保管方法	データセンタから自社オフィスのサーバへ1日 1 回遠隔バックアップ
	C.1.3.1	運用・保守性	通常運用	運用監視	監視情報	・データセンタのマネジメントサービスにより、死活監視、エラー監視、リソース監視を実施している。 ・社内からアプリケーションレベルでWebコンテンツのポーリングを定義実施している。
	C.1.3.2				監視間隔	リアルタイム監視(1 分間隔) データセンタのマネジメントサービスによる
	C.2.5.1		保守運用	定期保守頻度	定期保守頻度	定期保守を実施しない
	C.2.6.1			予防保守レベル	予防保守レベル	予防保守を実施しない
	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	復旧作業はすべて手動
	C.3.3.1			システム異常検知時の対応	対応可能時間	定額保守契約は締結していない
	C.3.3.2				駆けつけ到着時間	定額保守契約は締結していない
	C.3.3.3				SE到着平均時間	連絡がとれれば、遠隔操作で対応(定額保守契約はしていない)
	C.3.4.1			交換用部材の確保	保守部品確保レベル	確保しない
	C.3.4.2				予備機の有無	サーバおよびネットワーク機器に予備機あり
	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	通常の運用マニュアルに加え、復旧操作手順がある(社内で作成)
	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	データセンタ用に建築されたので、震度 7 相当まで耐えられる
	F.4.4.4			電気設備適合性	停電対策	データセンタは、自家発電装置により、1 日以上電源を確保することができる
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	全て従業員が実施する
	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	定額保守契約は締結していない
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	通常運用の訓練は実施しているが、復旧作業の訓練は実施していない
	C.5.9.1			定期報告会	定期報告会実施	実施していない

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
					頻度	
	C.5.9.2				報告内容のレベル	なし

Copyright © 2012 IPA, All Rights Reserved

(2)事例 2-2

業種・組織概要		
業種		地方公共団体
業務内容		行政サービス等の地方自治業務。
従業員数		5,000 名強。
検討対象の選定		
対象となるシステム基盤	重要業務	・住民窓口サービス(各種申請・届出等手続き、証明書発行業務等)
	業務選定の理由	・全庁の震災時対応を想定したBCPにおいて「優先すべき通常業務」の一つとして窓口業務が定められている。 ・なお、震災時対応を想定したIT-BCP では、職員間のコミュニケーションや住民等への情報提供を重要業務としている。
高回復力システム基盤構築の背景	経緯	・従前は汎用機により運用していた住民情報系基幹システムについて、オープン化を実施した。 ・公開を検討していた当時の汎用機は、障害も少なく運用が安定していた。オープン化しても同等の可用性を確保できるよう、システムの冗長化等を実施した。
	投資額の決定、経営者の関与等	・情報システム所管課長を中心に情報システム所管課内で個々の案件について検討し、統括情報化責任者(政策経営部門長)が決定を行っている。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO等)		[目標復旧時間(RTO)] ・規則等による定めはないが、4 時間(半日)程度。業務時間内には復旧することが求められる。 ・また、災害時には、全庁 BCP において、2 週間以内という目標復旧時間(RTO)が定められている。よって、住民情報系基幹システムも 2 週間以内に復旧することが求められる。 ・震災発生直後は、窓口業務に対する要求は少ない。しかし 2 週間ぐらい経過した段階では、証明書発行等の要望が発生する。 [目標復旧レベル(RLO)] ・規則等による定めはないが、通常時における処理能力の 50%程度 [目標復旧時点(RPO)] ・規則等による定めはないが、目標は障害発生時点。少なくとも前日の業務終了時点に復旧することが求められる。
高回復力システム基盤の概要	規模	・サーバ台数は約 20 台。 ・利用者数は約 500～600 人。
	システム構成と復旧対策の概要	・メインサイトでシステムを冗長化している。 ・住民情報は喪失することが許されないデータであるため、遠隔地へ月次でバックアップを送付している。現在は媒体保管を実施しているが、オンラインバックアップについても検討している。 ・システム構成の概要を図 3.3.2-2 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・メインサイト以外に、本庁に、ダウンリカバリシステムを設置している。メインサイトのサーバがダウンした場合に、証明書発行等、窓口サービスで重要な業務を継続できるような備えをしている。メインサイトのシステムとダウンリカバリシステムとの間では、日次でデータの同期をとっている。 ・他に、業務継続に向けた取り組みとして、サーバラックの免震化や、データセンタは浸水想定区域でもあるため、浸水対策も行っており、止水シートも配備している。
運用・見直しに関わる事項	震災時等の効果	・現システムについて、被災経験はない。
	将来構想	・今年度、費用削減の観点から、システムのあり方を精査する予定である。各システムの重要度と停止許容時間をもとに、冗長化の必要性を判断することを考えている。 ・WAN ネットワークの被害は不確定要素が大きいため想定するのは難しく、復旧に長時間を要する場合もあることから、ネットワークを利用せずに業務継続を図る方法も考えるべきだと考えている。例えば、本庁舎とデータセンタ間のネットワークが断絶したとしても、データセンタ内のサーバが無事な場合には、データセンタで住民への窓口業務を提供するといった方法も考えられる。

Copyright © 2012 IPA, All Rights Reserved

		・情報システムの復旧は職員だけでは対応できず、委託先事業者との連携が必須であるが、大震災が発生した場合に、支援を受けられるかどうかは不透明である。特に自設のデータセンタを利用しており、商用データセンタに比べると、支援が遅れることも懸念されるため、どのような対策を取るべきかが課題である。主要システムについては、災害時協力協定や、保守物品の提供に関する事前契約を結んでいるが、実際に委託先事業者が対応してくれるかどうかは不透明である。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.2-2 のとおり。		

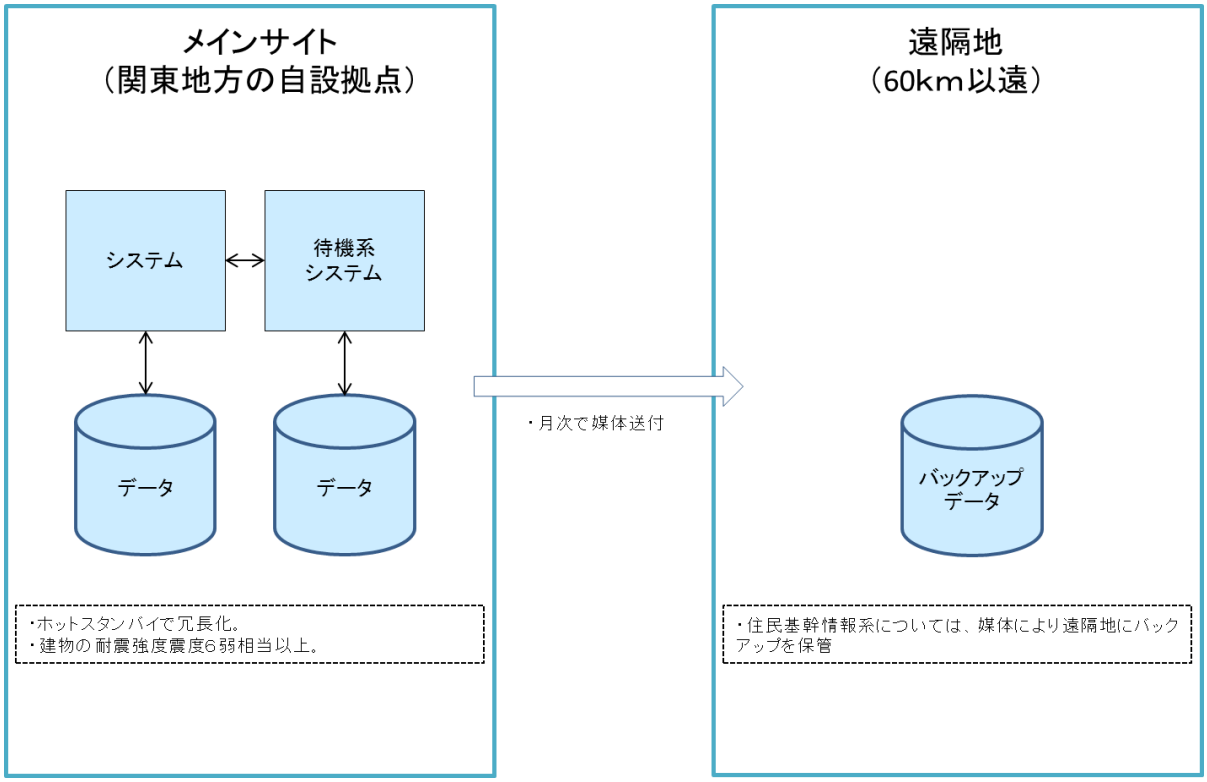

図 3.3.2-2 システム構成の概要

表 3.3.2-2 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	単一障害時には業務停止を許容せず処理を継続させる
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	障害発生時点
	A.1.3.2				RTO(目標復旧時間)	4 時間以内
	A.1.3.3				RLO(目標復旧レベル)	特定業務のみ
	A.1.4.1			目標復旧水準(大規模災	システム再開目標	1 か月以内

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
				害時)		
主要要件	A.2.1.1		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)	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)	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)	RAID1 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
	A.2.6.3				データインテグリティ	非回答
	A.3.1.1		災害対策	システム	復旧方針	限定された構成でシステムを再構築
	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、エラー監視、リソース監視、パフォーマンス監視を実施
	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	定期保守を実施しない
	C.2.6.1			予防保守レベル	予防保守レベル	監視システムにより検出している。報告は定例会にて実施
	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	重要な部分の障害復旧作業は自動化
	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、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する
	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	震度 6 弱相当
	F.4.4.4			電気設備適合性	停電対策	UPSにより、1時間程度電源を確保することができる
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	一部ユーザが実施
	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	規則等による定めはないが「システムの開発や構築に携わり、業務要件やユーザの事情にも通じている」対応者に期待している。
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	実施していない
	C.5.9.1			定期報告会	定期報告会実施	月 1 回

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
					頻度	
	C.5.9.2				報告内容のレベル	障害報告に加え運用状況報告を行う

Copyright © 2012 IPA, All Rights Reserved

3.3.3. モデルシステム 3 の事例

(1)事例 3-1

業種・組織概要		
業種		その他
業務内容		同一業界の複数企業が共同で利用するシステムの構築・運用等
従業員数		約 300 名
検討対象の選定		
対象となるシステム基盤	重要業務	・サービス利用者の契約者情報を管理するシステム。
	業務選定の理由	・災害時に参照される情報を提供する業務であり、停止すると社会的影響が大きいことから、重要業務とした。
高回復力システム基盤構築の背景	経緯	・1995 年の阪神・淡路大震災を機に当該システムに関連する業務の必要性を認識し、新規にシステムを構築した。その際、同時にバックアップサイトを構築した。
	投資額の決定、経営者の関与等	・費用は、システムを利用する各社が負担している。 ・方針の決定にあたっては、システムを利用している各社が構成員となっている委員会において実施している。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・目標は明確化していないが、大規模災害時にメインサイトが被害にあってもバックアップサイトで業務が継続できる必要があると考えている。
高回復力システム基盤の概要	規模	・メインサイトおよびバックアップサイトとも商用のデータセンタにメインフレームを設置し、同様の構成で構築している。
	システム構成と復旧対策の概要	・メインフレームを利用している。 ・メインサイトのデータは、月に 1 度、サービス契約者情報を更新し、その時点でのバックアップを MT(磁気テープ)保管し、バックアップサイトに陸送している。 ・バックアップサイトでは、メインサイトと同様の構成のシステムを用意し、非常時には利用できる状態で待機させている。 ・委託先事業者が管理するデータセンタ内にシステムを設置しており、保守員やSEが異常検知から数時間以内に駆け付けることが可能である。 ・バックアップデータは暗号化して保管している。 ・建物の耐震強度は震度 6 弱以上である。 ・システム構成の概要を図 3.3.3-1 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・本システムおよび関連する業務は、震災の混乱期においても、バックアップサイトにて円滑に業務を継続できた。これは、大規模地震が発生した場合の業務への影響を分析し、事業継続を行うための対策や対応手順を策定していたからだと考えられる。また、定期的に実施している演習や教育訓練も効果を発揮した
運用・見直しに関わる事項	震災時等の効果	・東日本大震災発生当時、メインサイトに目立った被害はなかったが、首都圏での大規模な余震の可能性を排除できなかったことから、バックアップサイトに切り替えた。切り替えは円滑に行われ、バックアップサイトにおいて正常に業務が行われた。
	将来構想	・東日本大震災の経験を通じて、システム対策の見直しには至らなかった。ただし、業務要件の観点から、収集すべき情報を見直す等の検討を行っている。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.3-1 のとおり。		

Copyright © 2012 IPA, All Rights Reserved

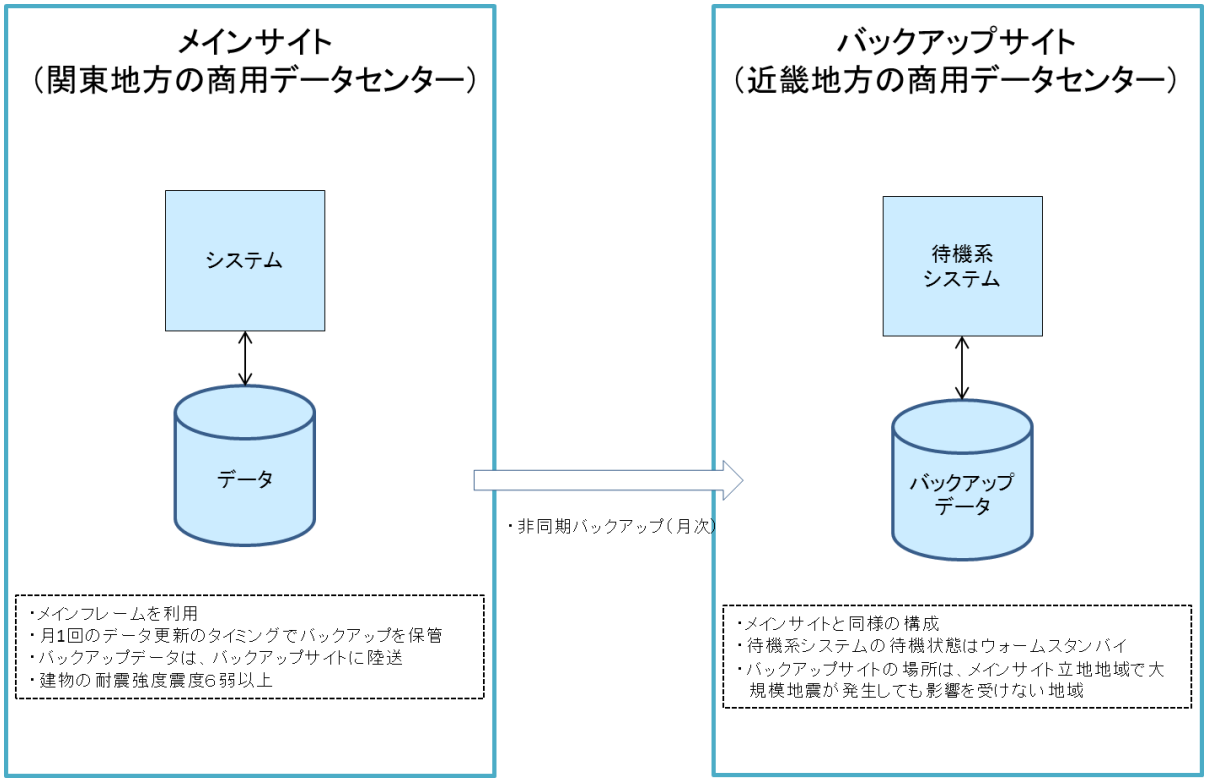

図 3.3.3-1 システム構成の概要

表 3.3.3-1 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	障害時の業務停止を許容する
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	障害発生時点
	A.1.3.2				RTO(目標復旧時間)	24 時間以上
	A.1.3.3				RLO(目標復旧レベル)	特定業務のみ
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	3 日以内に再開
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	ウォームスタンバイ
	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)	非冗長化
	A.2.3.2				冗長化(コンポーネント)	非冗長化
	A.2.4.1			ネットワーク	回線の冗長化	非冗長化
	A.2.4.2				経路の冗長化	非冗長化
	A.2.5.1			ストレージ	冗長化(機器)	特定の機器のみ冗長化
	A.2.5.2				冗長化(コンポーネント)	非冗長化
	A.2.5.3				冗長化(ディスク)	非冗長化

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
	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＆訂正)
	A.3.1.1		災害対策	システム	復旧方針	同一の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	遠隔地のバックアップサイトに保管
	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を実施
	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	週 1 回
	C.2.6.1			予防保守レベル	予防保守レベル	(定期保守とは別に)一定間隔で予兆検出を行い、対応を行う
	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	障害復旧作業はすべて手動
	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	保守契約に基づく規定年数の確保
	C.3.4.2				予備機の有無	一部、予備機あり
	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する
	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	震度 6 弱相当
	F.4.4.4			電気設備適合性	停電対策	CVCF・UPSの導入、電源の 2 系統化、重油の優先確保を行っている。
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	全てベンダが実施
	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	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	通常運用に加えて保守運用の訓練を実施
	C.5.9.1			定期報告会	定期報告会実施頻度	四半期に 1 回
	C.5.9.2				報告内容のレベル	障害および運用状況報告に加えて、改善提案を行う

Copyright © 2012 IPA, All Rights Reserved

(2)事例 3-2

業種・組織概要		
業種		サービス業
業務内容		受託業務を中心としたサービス業の持株会社
従業員数		約 2,000 名(グループ連結) 約 50 拠点(グループ連結/国内・海外拠点含む)
検討対象の選定		
対象となるシステム基盤	重要業務	・ERPシステム(財務会計・人事管理・販売管理・ワークフロー)等で扱う基幹業務。(以降特に断りが無い限りはERPシステムに関する記載とする。) ・メール・グループウェア等のコミュニケーション業務
	業務選定の理由	・持株会社として各事業会社を横断的に統括しているため、グループ全体として事業継続性や連結決算対象として見た場合に影響のある業務を選定した。
高回復力システム基盤構築の背景	経緯	・震災直後、当時サーバ設置していたビルが計画停電対象地域に含まれており、全サーバを停電の影響を受けにくいデータセンタへ移設する検討を開始した。
	投資額の決定、経営者の関与等	・ITに関しては、IT統括部門で検討・策定した内容をリスク管理委員会で協議・決定し、実現する流れとなっている。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・経営層からは、リアルタイムの同期バックアップを実現するようにという指示があった。これに対して、実現に必要な費用を勘案し、事業継続の観点から必要な目標を再検討して現在の構成に決めた。
高回復力システム基盤	規模	・サーバ台数(1 拠点あたり):ブレードサーバ 24 台(通常稼働している 18 台に加え残りは予備) ・利用拠点数:2 拠点(メインサイト:近畿地方、バックアップサイト:関東地方) ・利用人数:2,400 ユーザ
	システム構成	・メインサイトとバックアップサイトは同一構成であり、ウォームスタンバイ構成である。 ・データは夜間自動的に日次バックアップしている。 ・各サイト内でのシステムの二重化はしていない。 ・各拠点(50 箇所)は、インターネット回線やモバイル環境にて接続している。VPN で接続している箇所もある。 ・もともと本社にあったサーバを震災後に近畿地方のデータセンタに移設し、その後、関東地方のデータセンタに待機系システムを構築した。

Copyright © 2012 IPA, All Rights Reserved

の概要	と復旧対策の概要	・待機系システムとの切り替えは、経営判断を伴うため手動で切り替えを実施する。具体的には DNS の設定を変更する。 ・メインサイト復旧後も元のシステム形態に戻すことはなく、バックアップサイトでそのまま業務を継続することとしている。(同じ環境であるため業務上制約は無く、戻すリスクの方が大きいと判断した。) ・今年は、関西電力管内で計画停電の可能性があるため、関東地方のデータセンタをメインサイトにすることを検討している。 ・システム構成の概要を図 3.3.3-2 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・3 つの実現パターン(バックアップサイトにて同期バックアップ、現在の構成、遠隔バックアップのみ)を比較検討した。バックアップサイトにて同期バックアップを実現する案は費用がかかりすぎるため、実現しなかった。遠隔バックアップでは、監査法人が要求するIT 統制に関わる要件を満足できないと判断し、現在の構成とした。 ・ERP以外のシステムも一部を除き殆ど全てデータセンタに設置または、クラウドサービスに移行した。現在ERPシステムを任せている委託先事業者と、それ以外のシステムを任せている委託先事業者の 2 社にフルアウトソーシングしている。これにより、データセンタ利用料等の委託先事業者に支払うコストは以前より増加したが、社員の負担は大幅に軽減された。
運用・見直しに関わる事項	震災時等の効果	・東日本大震災発生当時は現在のシステム構成では無かったが、今後は関東と関西で同時に大規模災害や長期停電に見舞われない限り業務継続が可能となる。
	将来構想	・現在は仮想化サーバと通常のサーバが稼働しているため、今後は全て仮想化環境に統一することも考えられる(現在、プロキシやリモートアクセス等の共通基盤は仮想化環境で稼働している)。 ・ERPシステムを委託している委託先事業者と、メール・グループウェア等のシステムを委託している委託先事業者の 2 社による体制は、委託先事業者の長所も踏まえた適材適所のベストチョイスと認識している。この先しばらくは変わらないと考えている。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.3-2 のとおり。		

Copyright © 2012 IPA, All Rights Reserved

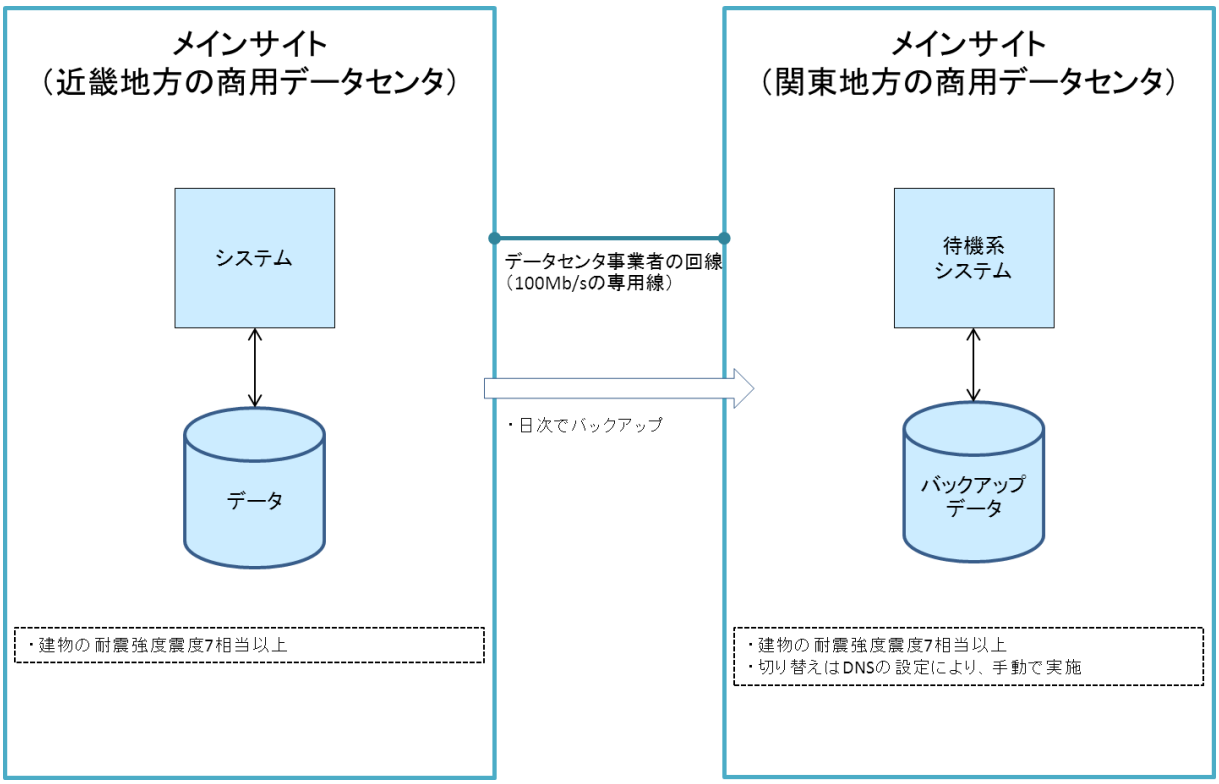

図 3.3.3-2 システム構成の概要

表 3.3.3-2 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	障害時の業務停止を許容する
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	日次バックアップからの復旧
	A.1.3.2				RTO(目標復旧時間)	数時間以内
	A.1.3.3				RLO(目標復旧レベル)	ERPの全ての業務
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	3 日以内に再開
主要要件	A.2.1.1		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)	全てのコンポーネントを冗長化
	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)	全てのコンポーネントを冗長化
	A.2.4.1			ネットワーク	回線の冗長化	データセンタと本社間を冗長化
	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(バックアップサイト)
	A.2.5.2				冗長化(コンポーネント)	一部冗長化

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
	A.2.5.3				冗長化(ディスク)	RAID5 以上による冗長化
	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＆訂正)
	A.3.1.1		災害対策	システム	復旧方針	同一の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	遠隔地のバックアップサイトに保管
	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、エラー監視、リソース監視を実施
	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する
	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	復旧作業はすべて手動
	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	データセンタ内に保守要員が常駐
	C.3.3.3				SE到着平均時間	データセンタからSEへ連絡し、リモートで対応。
	C.3.4.1			交換用部材の確保	保守部品確保レベル	保守契約に基づく規定年数の確保
	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する
	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	データセンタなので震度7相当
	F.4.4.4			電気設備適合性	停電対策	自家発電装置により、約3日間電源を確保することができる
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	全てベンダが実施
	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	導入に関わったSEが対応している
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	実施していない
	C.5.9.1			定期報告会	定期報告会実施頻度	月1回
	C.5.9.2				報告内容のレベル	障害および運用状況報告に加えて、改善提案を行う

Copyright © 2012 IPA, All Rights Reserved

3.3.4. モデルシステム 4 の事例

(1)事例 4-1

業種・組織概要		
業種		サービス業
業務内容		工業製品の品質、安全性検査や認証等
従業員数		約 300 名
検討対象の選定		
対象となるシステム基盤	重要業務	・最重要業務は、検査や認証等の管理業務である。 ・なお、構築しているシステム基盤には、経理関係等の社内向けのシステムを除き、ほとんどの業務システムが搭載されている。
	業務選定の理由	・ITディザスタリカバリープランにおいて、システムの優先順位づけは決定されている。最も重要な業務は顧客への製品の認証に関する情報提供(オンラインのデータベースサービス)である。この情報がないと、お客様は製品の生産や販売することができない。止めることが許されないサービスである。 ・このため、検査や認証情報等の提供については、顧客と SLA を設定して契約している。当社としても、SLA を遵守しペナルティが発生しないよう、検査や認証等の管理業務の復旧優先順位は確実に高く保つ必要がある。
高回復力システム基盤構築の背景	経緯	・コスト、予算、顧客の要望等いろいろと要因はあるが、サーバ統合・集約化プロジェクトのスタートが契機となり、あわせてシステムの復旧対策を実現した。 ・構築のために、相当のコストがかかったが、運用はコストが削減された。現在の運用要員人数は、メインサイトとバックアップサイトの拠点に各 1 名ずつである。以前は各拠点に分散していたので、運用要員が 5～6 人必要であった。あわせて、サーバ台数も縮減できた。
	投資額の決定、経営者の関与等	・ITサービスの対策レベルは、当該業務で確保できる予算規模で決定される。業務の優先順位を社長が決定することは基本的にはないが、予算配分を決定する際に、結果的に社長と CFO が判断することはある。 ・バックアップサイトの投資額については、震災発生当時のバックアップサイトの構築には、本社のサイトを1.0 とすると 0.3 ほどの費用が発生した。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		・目標復旧時間(RTO)は、最も高水準のサービスで 5 分である ・個々の顧客との契約(SLA)に応じて、契約単位で目標復旧時間(RTO)を設定している。 ・目標復旧時間(RTO)を 5 分より短くすると、大幅に費用(投資費用とそれに見合う顧客に請求する料金)が増加するため現実的ではないと判断し、最も高水準のもので5分と設定した。 ・目標復旧レベル(RLO)、目標復旧時点(RPO)は設定していない。 ・このような内容は、社長は直接判断に関与しない。IT部門は、業務部門からの要求に基づいて対策を検討して、予算の範囲内で対応する。
高回復力システム基盤の概要	規模	・本社のサーバは、4 台のブレードサーバを 2 セット用意しクラスタ構成にしている。
	システム構成と復旧対策の概要	・メインサイトは仮想化技術を導入し、クラスタ構成により冗長化している。 ・バックアップサイトもメインサイトとほぼ同様の構成となっている。 ・メインサイトとバックアップサイト間は 100Mb/s の専用線で結ばれ、ストレージベースのレプリケーション機能の活用により最短 5 分でデータ同期している。 ・仮想化技術を活用したバックアップサイトを構築し、最短 5 分で切り替え処理可能。 ・システム構成の概要を図 3.3.4-1 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・システムの統合作業とバックアップサイトの設置を同時に進めることにより、サーバ台数を削減しシステム運用の効率性を高めるとともに、ITサービスの継続性を確保した。
運用・見直しに関わる事項	震災時等の効果	・震災時、本社のサイトは特に被害はなかったが、安全性を確保するにあたり、念のため、バックアップサイト(関西圏)に、150VM(仮想マシン)中、15VM の切り替え処理を実施した。この際、システムの再立ち上げや管理者の確認を含め、作業は 30 分で完了した。 ・本来の運用形態に戻す処理には 2 週間ほど要した。データを最新化するのに時間を要したためである。当時本来の運用形態に戻す処理の経験や標準手順が確立していなかった。現在は手順を定め、方法が確立したので、1 週間程度で実施可能である。なお、本来の運用形態に

Copyright © 2012 IPA, All Rights Reserved

		戻す処理を実施するタイミングは特に決めず、顧客の要望や技術的条件などにより決定する。
	将来構想	・今後は、災害時、バックアップサイトの起動は、メインサイトではなく、バックアップサイト側で起動する。これは、バックアップサイトを起動するときはメインサイトが被災している可能性があるため、バックアップサイト側でコントロールした方がよいと考えたからである。 ・さらに、将来的には世界 3 か所(ヨーロッパ、アジア、米国)のデータセンタにシステムを集約し、相互にバックアップする仕組みを備える構想を描いている。 ・海外のデータセンタを開設した場合は、情報セキュリティ対策が難しくなると予想される。データの保護や、情報セキュリティに関する契約について海外については国内とは異なる検討が必要となる。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.4-1 のとおり。		

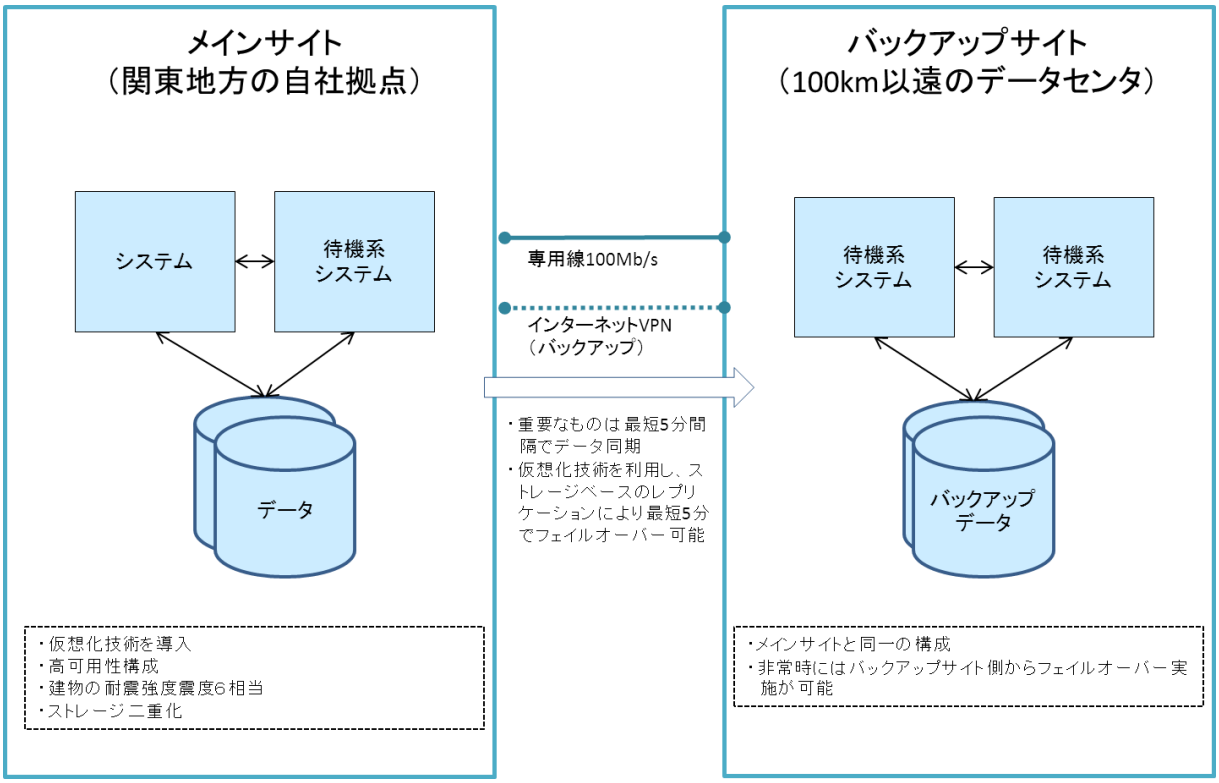

図 3.3.4-1 システム構成の概要

表 3.3.4-1 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	単一障害時には業務停止を許容せず処理を継続
	A.1.3.1			目標復旧水準（業務停止時）	RPO(目標復旧時点)	未設定
	A.1.3.2				RTO(目標復旧時間)	5 分
	A.1.3.3				RLO(目標復旧レベル)	未設定

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	1 日以内
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	全てのサーバで冗長化と同等(仮想化技術を活用)。
	A.2.1.2				冗長化(コンポーネント)	全てのコンポーネントを冗長化
	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)	電源・FAN 等は冗長化されている
	A.2.4.1			ネットワーク	回線の冗長化	WAN は専用回線に加えバックアップ回線としてインターネット VPN を利用している
	A.2.4.2				経路の冗長化	LAN・WAN 回線ともに 2 重化され 1 か所で障害が発生しても、通信が可能な構成となっている。
	A.2.5.1			ストレージ	冗長化(機器)	ストレージ 2 台構成
	A.2.5.2				冗長化(コンポーネント)	一部のコンポーネントを冗長化
	A.2.5.3				冗長化(ディスク)	RAID-DP 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
	A.2.6.3				データインテグリティ	ハッシュ関数を利用したエラー検出と再試行
	A.3.1.1		災害対策	システム	復旧方針	本番サイトとほぼ同等の構成をバックアップサイトに設置
	A.3.2.1			外部保管データ	保管場所分散度	100km 以遠のデータセンタがバックアップサイトとなっている。
	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、エラー監視、リソース監視、パフォーマンス監視を実施
	C.1.3.2				監視間隔	リアルタイム監視(1～2 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	監視システムにより、故障の予兆状況を検出
	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	すべて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	原則 3 時間以内
	C.3.3.3				SE到着平均時間	原因を自社で調査し、問題個所特定後 3 時間以内
	C.3.4.1			交換用部材の確保	保守部品確保レベル	特定の機種のみ、例外的にシステム専用の部品を確保
	C.3.4.2				予備機の有無	ブレードサーバの予備機が有り
	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が提供されている
	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	1981 年以降の建築物なので、震度 6 強にも耐えられる。
	F.4.4.4			電気設備適合性	停電対策	非回答

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	一部ユーザが実施する
	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	非回答
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	非回答
	C.5.9.1			定期報告会	定期報告会実施頻度	非回答
	C.5.9.2				報告内容のレベル	非回答

Copyright © 2012 IPA, All Rights Reserved

(2)事例 4-2

業種・組織概要		
業種		サービス業
業務内容		金融商品取引業務
従業員数		約 850 名
検討対象の選定		
対象となるシステム基盤	重要業務	・金融商品取引業務
	業務選定の理由	・システムでしか行えない業務であり代替手段が無いため。
高回復力システム基盤構築の背景	経緯	・高速性(応答性能 2 ミリ秒)、拡張性(あらかじめ定めた拡張基準を超えた場合、1 週間程度で対応を可能)、信頼性(99.999%以上の可用性)等を達成するために、様々な議論を重ね、現在の構成となった。
	投資額の決定、経営者の関与等	・IT企画・検討及び運用・管理は情報システム部門が実施。施策は、社長及び役員が意思決定している。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO等)		・目標復旧時間(RTO)は、ハードウェア故障時は 0 分である。大規模災害時は取引業務:24 時間以内を復旧目標としている。 ・目標復旧レベル(RLO)については、定量的な基準として設定しているものはない。各部で目標レベルを定めているが、定性的な内容となる。 ・目標復旧時点(RPO)については、障害発生直前である。
高回復力システム基盤の概要	規模	・メインサイト:200 台 ・取引処理件数:60 万件/分
	システム構成と復旧対策の概要	・メインサイトとバックアップサイト間でリアルタイムにバックアップを実施している。 ・バックアップサイトはウォームスタンバイである。通常は、開発用としても使用しており、手動による切り替えを行う。 ・サーバは三重化構成である。 ・ネットワークは二重リング構成である。(一部が切断しても、利用継続可能な構成) ・システム構成の概要を図 3.3.4-2 に示す。
導入にあたって		
構築にあたってのポイントや留意点		・レスポンスを重視するため、データ処理は全てメモリ上で行い、ディスクへの書き込みは随時行わない方式をとっている。 ・信頼性を確保するため、サーバは三重化構成をとっている。 ・レスポンス重視だが、DBMS を含め一般的な市販製品を採用している。システム自体がビジネスであるため、競争力を高めるためにはシステムコストの最小化を図ることが必要である。
運用・見直しに関わる事項	震災時等の効果	・震災による直接被害は無かった。
	将来構想	・首都直下地震を想定した対応の検討を今後行う。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.4-2 のとおり。		

Copyright © 2012 IPA, All Rights Reserved

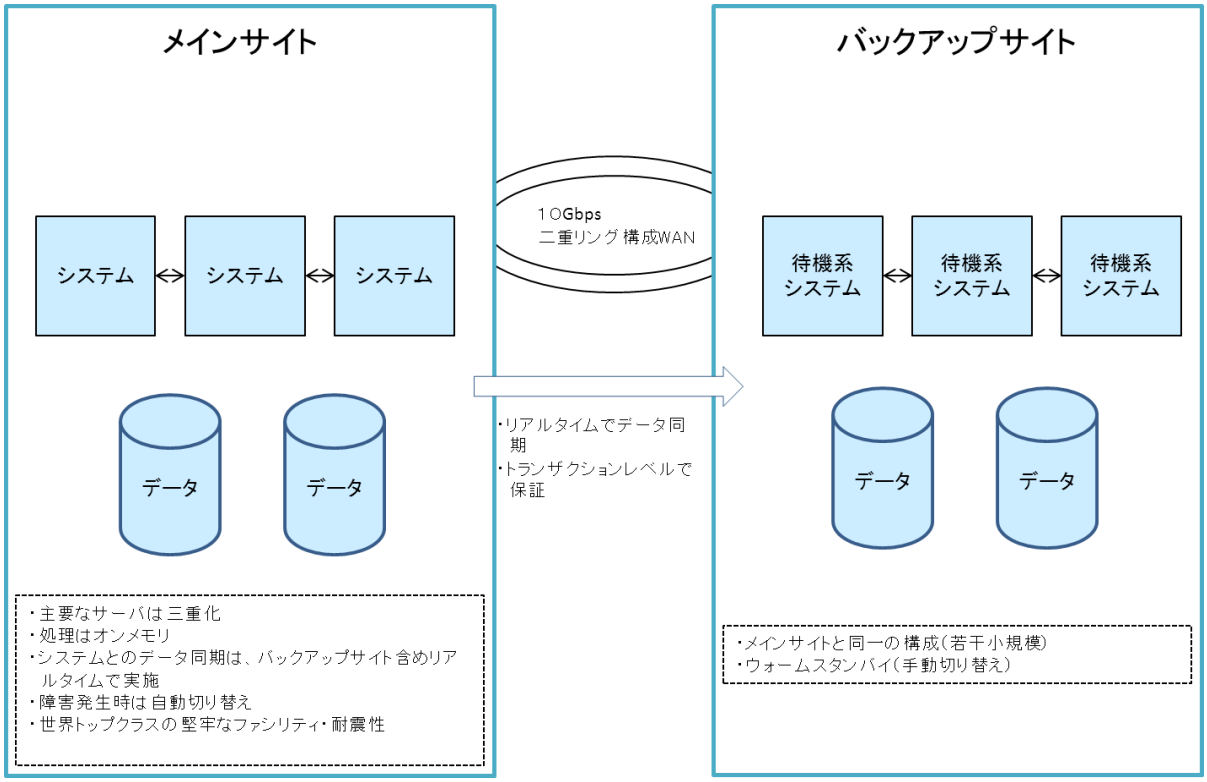

図 3.3.4-2 システム構成の概要

表 3.3.4-2 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	稼働率を 99.999%以上と設定している(5 年間で 10 分程度の停止時間)
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	障害発生時点(トランザクション単位)
	A.1.3.2				RTO(目標復旧時間)	ハードウェア故障時は停止時間 0 分
	A.1.3.3				RLO(目標復旧レベル)	各部で定性的な目標レベルを定めている程度
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	24 時間以内復旧
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	主要な全てのサーバで冗長化(三重化)
	A.2.1.2				冗長化(コンポーネント)	全てのコンポーネントを冗長化
	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)	全てのコンポーネントを冗長化
	A.2.4.1			ネットワーク	回線の冗長化	・基幹網は二重リング構成(自前回線) ・アクセス回線はキャリアサービス(2 か所のアク

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
						セスポイントに接続)
	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)	全て冗長化
	A.2.5.2				冗長化(コンポーネント)	全て冗長化
	A.2.5.3				冗長化(ディスク)	全て冗長化
	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
	A.2.6.3				データインテグリティ	非回答
	A.3.1.1		災害対策	システム	復旧方針	メインサイト・バックアップサイトとも構成はほぼ同一
	A.3.2.1			外部保管データ	保管場所分散度	遠隔地のバックアップサイトに保管
	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、エラー監視、リソース監視、パフォーマンス監視を実施
	C.1.3.2				監視間隔	リアルタイム監視(最短は1秒間に 1 回)
	C.2.5.1		保守運用	定期保守頻度	定期保守頻度	定期保守は実施しない(エラー監視はシステムで実施しており不要)
	C.2.6.1			予防保守レベル	予防保守レベル	監視システムにより、故障の予兆状況をほぼリアルタイムで検出
	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	・同一サイト内の切り替えは自動化されている。 ・バックアップサイトは手動切り替え。
	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 24 時間常駐
	C.3.3.3				SE到着平均時間	システムサービス時間内は常駐(時間外は呼び出し)
	C.3.4.1			交換用部材の確保	保守部品確保レベル	システム専用の部品を特別に確保している。予備部品は保守委託先事業者拠点に保有。原則全部品あり。
	C.3.4.2				予備機の有無	予備部品は無い(三重化のため不要)
	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	緊急時対応を含めたカスタマイズされたマニュアルを準備している
	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	世界トップクラスの堅牢なファシリティ・耐震性。
	F.4.4.4			電気設備適合性	停電対策	自家発電装置を設置(電源確保可能時間は非回答)
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	従業員(運用担当)および運用委託先事業者(運用オペレータ)が常駐し一次対応を行う
	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	現状、オペレータには業務関する判断は行わせていない。
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	運用委託先事業者、構築委託先事業者、顧客も参加して訓練を実施している
	C.5.9.1			定期報告会	定期報告会実施頻度	月 1 回
	C.5.9.2				報告内容のレベル	故障報告・運用報告に加え、改善策提案も報告している

Copyright © 2012 IPA, All Rights Reserved

(3)事例 4-3

業種・組織概要		
業種		食品製造業
従業員数		150 名
事業拠点		本社拠点 3、営業所 5、出張所 2 拠点
検討対象の選定		
対象となるシステム基盤	重要業務	・製造・販売・管理業務(対応システム:製造・販売・管理システム) ・顧客とのコミュニケーション(対応システム:メール等の情報系システム)
	業務選定の理由	・製造・販売管理業務や顧客とのコミュニケーション機能が停止すると、「お客様第一主義(お客様へのサービスレベルを維持する)」という社の方針に沿えないこと、商品を製造・販売できなくなることから売上(利益)が確保できなくなるからである。 ・情報システム部門が企画・検討を行い、CIO によって意思決定を行い決定した。
高回復力システム基盤構築の背景	経緯	・過去に起きた水害によりサーバが水没した経験がある。当時、机の上にサーバを退避させたが、机の上まで水が上がった。これは想定していなかった事態であった。 ・この経験の教訓として、事業継続にはデータが重要性であることを CIO が認識し、遠隔地にバックアップ環境を構築することが命題となり、現在のシステムを導入する契機となった。 ・ただし、バックアップ環境構築の点のみでシステム構築を実施した訳ではない。全体最適の観点でシステム再構築を行った結果、最適化とバックアップ環境の両面が同時に実現できた。
	投資額の決定、経営者の関与等	・ハードウェアの更改時に全サーバをブレードサーバ化することも検討したが、数千万の費用がかかることが判明した。ブレードサーバ化せず、仮想化環境を構築する場合は、既存サーバを利用することが可能であり、費用も仮想化を行わずハードウェアを更改した場合と同等以下であったため導入に至った。
対象システムの概要		
対象となるシステム基盤で稼働する業務の事業継続戦略(RTO 等)		[目標復旧時間(RTO)] ・目標復旧時間(RTO)は未設定である(設定の予定なし)。 ・理由は、現在構築したシステムは、ほぼリアルタイムに復旧可能であり、これ以上に求める目標はないため、特に定める必要はないと考えているからである。 [目標復旧レベル(RLO)] ・目標復旧レベル(RLO)は未設定(検討中)であるが、通常時よりも低いレベル(たとえば伝票の打ち出しが遅くなるなど)でも出荷業務が可能なレベルであればよいと考えている。 [目標復旧時点(RPO)] ・目標復旧時点(RPO)は未設定(検討中)である。
高回復力システム基盤の概要	規模	・サーバ数:計 7 台(クラスタ構成・仮想化 6 台・バックアップサイト 1 台) ・クライアント端末数:150 台(うち 50 台を仮想デスクトップ化)
	システム構成と復旧対策の概要	・本番サイトとバックアップサイト間でリアルタイムバックアップを実施。 ・切り替え処理は、メインサイトのサーバがダウンすると DNS のサーバアドレス更新が行われ、クライアント端末を再起動すれば、バックアップサイトにつながる仕組みである。数秒で切り替えが可能である。 ・本来の運用形態に戻す処理も、管理画面から簡単に実施できる。 ・ネットワークはインターネット VPN 環境を構築している。 ・今回メインサーバ環境 2 台とバックアップサイトのサーバ 1 台は既存サーバを流用し仮想化技術で構築しため、大きな費用はかかっていない。 ・システム構成の概要を図 3.3.4-3 に示す。
	技術的特徴<導入した技術・サービスの内容>	・仮想化技術を導入(クラスタ構成のサーバによる全システムの仮想化、クライアント端末は VDI(Virtual Desktop Infrastructure)方式の仮想化)。
導入にあたって		
構築にあたってのポイントや留意点		・仮想化技術の採用は、以下のような非常に大きいメリットがあった。 〇サーバ統合化によりコストの削減と運用負担の軽減が図れた。 〇バックアップサイトを構築することにより、事業継続性の強化が実現できた。

Copyright © 2012 IPA, All Rights Reserved

		○クラスタ化された仮想サーバ構成を構築したため、ハードウェア障害に強くなった。 ○また、エンドユーザの業務に影響を与えずに(システムを止めずに)、修理やメンテナンス等の保守作業が可能となった(仮想サーバの機能を活用)。 ○保守面においても、ネットワークを介した遠隔地での検証作業や保守・サポートが可能な環境としたため、対応も早く、効率的である(これまでは物理サーバに対し、駆けつけ保守やセンドバック保守を行っていた)。 ○デスクトップの仮想化により、クライアント端末の復旧スピードの向上とともにメンテナンス負担が大幅に軽減できたとともに、VDI 方式の導入によりレスポンスも早くなっている。 ・ただし、仮想化については、サーバのサイジングがむずかしかった。50 台のデスクトップ環境を動作させ、検証を繰り返した。
運用・見直しに関わる事項	震災時等の効果	・本システムを導入してから、災害は発生していない。
	将来構想	・IT-BCP に関して、ネットワークの冗長化を検討している。
対策例		
高回復力システム基盤の要件と対策(要件内容)は表 3.3.4-3 のとおり。		

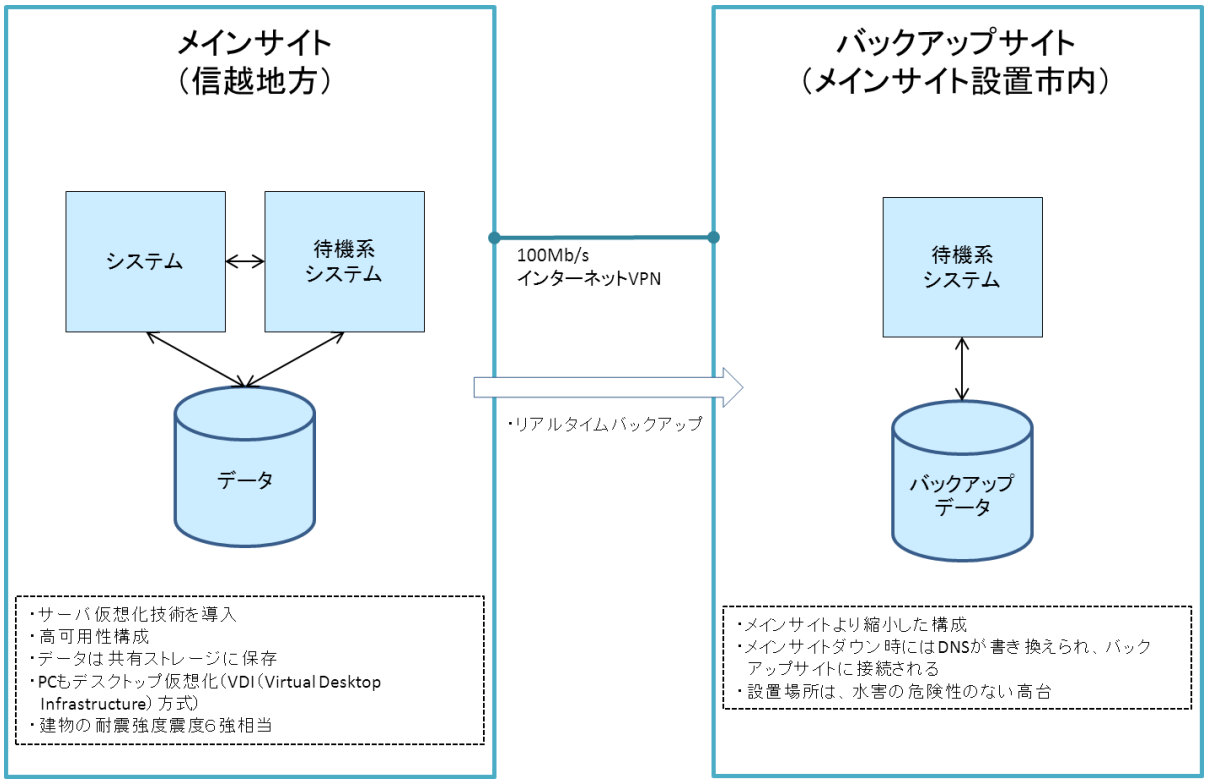

図 3.3.4-3 システム構成の概要

Copyright © 2012 IPA, All Rights Reserved

表 3.3.4-3 高回復力システム基盤の要件と対策(要件内容)

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
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	二重障害時には停止を許容。ただし、複数台のサーバで仮想化環境が用意されているため、代替するシステムの稼働環境を用意することは可能。
	A.1.3.1			目標復旧水準(業務停止時)	RPO(目標復旧時点)	障害発生時点
	A.1.3.2				RTO(目標復旧時間)	定めていないが、現状のシステムでは、ほぼ 0 時間である
	A.1.3.3				RLO(目標復旧レベル)	・特定の業務。 ・性能は低い水準を許容。
	A.1.4.1			目標復旧水準(大規模災害時)	システム再開目標	・全域災害の場合や人的被害が大きい場合は運用・保守人員の確保が困難であるため再開不能。 ・そうでない場合、データがあれば 3 日以内に再開可能。
主要要件	A.2.1.1		耐障害性	サーバ	冗長化(機器)	・デスクトップ仮想化については、クラスタ構成による三重化(サーバ3台)。 ・それ以外は冗長化。
	A.2.1.2				冗長化(コンポーネント)	・ディスク、ネットワークカードは冗長化。 ・電源等は冗長化していない。
	A.2.3.1			ネットワーク機器	冗長化(機器)	非冗長化
	A.2.3.2				冗長化(コンポーネント)	非冗長化
	A.2.4.1			ネットワーク	回線の冗長化	非冗長化
	A.2.4.2				経路の冗長化	非冗長化
	A.2.5.1			ストレージ	冗長化(機器)	非冗長構成(バックアップサイトにより冗長化しているという考え)。
	A.2.5.2				冗長化(コンポーネント)	電源、FAN は冗長化している
	A.2.5.3				冗長化(ディスク)	RAID5 以上
	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
	A.2.6.3				データインテグリティ	エラー検出及び再試行を実施。
	A.3.1.1		災害対策	システム	復旧方針	本サイトより小さな構成でバックアップサイトを構築
	A.3.2.1			外部保管データ	保管場所分散度	市内の別拠点(高台)1 ヵ所に保管
	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	・システム機能としてはパフォーマンス監視の確認は可能。運用上はパフォーマンス低下時など、必要に応じて確認を実施。 ・死活監視は全サーバ毎日実施。
	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	アラートが生じた場合のみ実施、定期的な保守は行っていない
	C.2.6.1			予防保守レベル	予防保守レベル	監視システムにより、故障の予兆状況を検出
	C.3.2.1		障害時運用	障害復旧自動化の	障害復旧自動化の範囲	・バックアップサイトへの切り替えは自動化(自動で DNS の切り替え実施)。

Copyright © 2012 IPA, All Rights Reserved

分類	項番	大項目	中項目	小項目	要件	対策(要件内容)
				範囲		・クライアント端末は再起動すれば新しい DNS 設定が有効となり、ミラーサーバへの切り替えが行われる。 ・なお、デスクトップ仮想化環境サーバがダウンした場合には、基幹システムのクライアント端末は通常の PC として動作させることも可能。
	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	数時間内
	C.3.3.3				SE到着平均時間	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	保守契約に基づく規定年数の確保
	C.3.4.2				予備機の有無	・ネットワーク機器、クライアント端末は予備機有り。 ・サーバはリプレース前のものを予備機としている。
	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	・各製品のマニュアルを利用。 ・運用手順書、マニュアル等はない。
	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	1981 年以降の建設であり、震度 6 強にも耐えられる
	F.4.4.4			電気設備適合性	停電対策	自家発電装置により、40 時間電源を確保することができる
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	一部ユーザが実施する
	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	・特に明文化はしていない。 ・対応者は、提案を含め利用環境を構築してきた担当者が対応。
	C.5.8.2			オペレーション訓練	オペレーション訓練範囲	・サーバ切り替えの訓練は実施していない。(導入時にテストを実施)。
	C.5.9.1			定期報告会	定期報告会実施頻度	実施していない
	C.5.9.2				報告内容のレベル	なし

Copyright © 2012 IPA, All Rights Reserved

4. 高回復力システム基盤構築におけるクラウドサービスの活用

4 章では高回復力システム基盤に有用と思われるクラウドサービス例を紹介するとともに、クラウドサービスを利用する留意点について説明する。

4.1. 高回復力システム基盤に有用と思われるクラウドサービス例

「情報システム基盤の復旧に関する対策の調査」のうち「新しい技術・サービス」に関する文献調査において、東日本大震災で被災した組織がクラウドサービスなどを利用して業務を行った事例が多くあることがわかった。また、事例調査結果からは、震災をきっかけとして、データバックアップやバックアップサイト構築を目的としてクラウドサービスを活用しようとする動きが見られた。

高回復力システム基盤の実現のために、遠隔地にデータ保管先を確保、あるいはバックアップサイトを構築するための用地、施設設備、機器等を自前で調達するには、相応の初期投資が必要となる。

コスト(投資)面の制約により自前で上記のような対策実施が難しいと考えている組織にとって、クラウドサービスの活用は、有用な選択肢となっている。

モデルシステム 1～4 のような高回復力システム基盤導入に有用なクラウドサービスの活用形態は、以下の 2 つに大別できる。

・データの遠隔地バックアップ先としてクラウドサービスを利用する(モデルシステム 1、2 に対応)
・バックアップサイトの構築先としてクラウドサービスを利用する(モデルシステム 3、4 に対応)

Copyright © 2012 IPA, All Rights Reserved

4.1.1. データの遠隔地バックアップ先としてクラウドサービスを利用する

バックアップデータをクラウド上のストレージに保管する。モデルシステム 1、2 に対応するクラウドサービスの活用例である。

(1)メインサイトは自社施設、外部データセンタ利用、クラウドサービス利用のいずれでもよいが、自前以外の場合は、データセンタ事業者やクラウド事業者の方針や環境等によって、実現の可否や方法が左右される。

(2)遠隔地バックアップのためのクラウドサービス利用形態には、以下のようなものがある。

①クラウド事業者が提供するストレージを用いて、ユーザ自身が構築・運用する。

②クラウド事業者が提供するバックアップサービスを利用する。メインサイト側にエージェントを導入する必要があるもの、クラウドサービス側のエージェントが自動的にバックアップ対象にアクセスするもの等、幾つか種類がある。クラウドサービス側データセンタの所在がメインサイトから見て「適切な遠隔地」(同一災害により影響を受けない等)であること、および契約により大規模災害時のデータ保全が担保されることを確認する必要がある。

システム構成イメージを下図に示す。

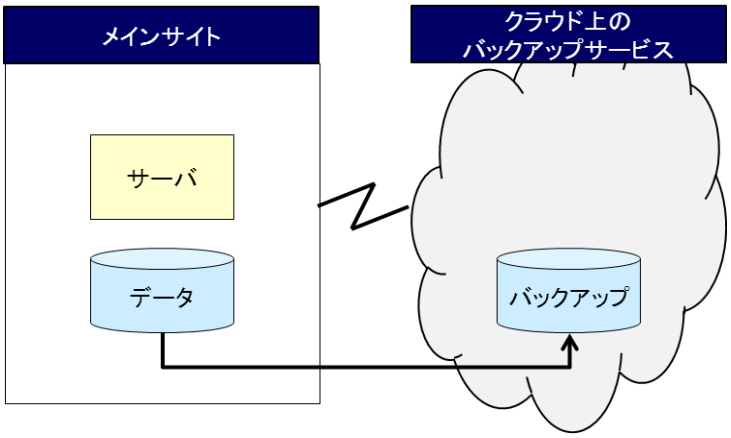

図 4.1.1-1 バックアップデータをクラウド上に保管するイメージ

主要要件「A.3.2.2 可用性 / 災害対策 / 外部保管データ / 保管方法」について、モデルシステム 1、2 にあらかじめ設定された要件内容は「媒体による保管」であるが、クラウドサービスを利用することにより、モデルシステム 3、4 と同等の「バックアップサイトへリモートバックアップ」のリモートバックアップを実現する。

Copyright © 2012 IPA, All Rights Reserved

4.1.2. バックアップサイトの構築先としてクラウドサービスを利用する

バックアップサイトをクラウド上に構築する。モデルシステム 3、4 に対応するクラウドサービスの活用例である。メインサイトが停止した際にはバックアップサイトに切り替えて業務を再開させる。この場合の目標復旧時間(RTO)は、メインシステム停止からクラウド側でのサービス開始までの所要時間を表す。

(1)メインサイトは自社施設、外部データセンタ利用、クラウドサービス利用のいずれでもよいが、自前以外の場合は、データセンタ事業者やクラウド事業者の方針や環境等によって、実現の可否や方法が左右される。
(2)バックアップサイトはクラウド事業者が提供するサービスを利用してユーザ自身が構築・運用する。
クラウドサービス側データセンタの所在がメインサイトから見て「適切な遠隔地(同一災害により影響を受けない等)」であること、および契約により大規模災害時の機能およびデータ保全が担保されることを確認する必要がある。

システム構成イメージを下図に示す。

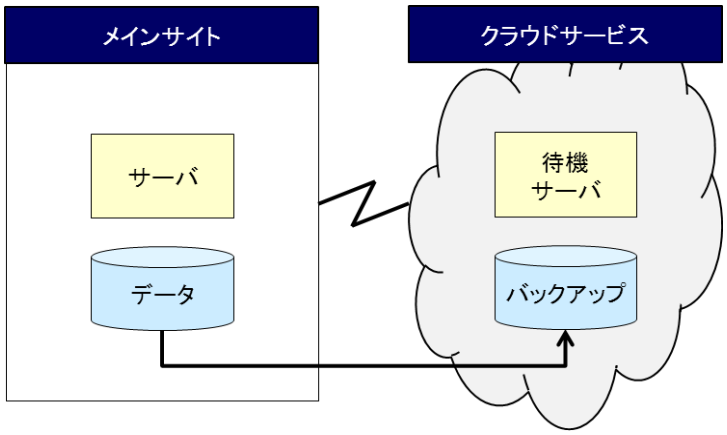

図 4.1.2-1 バックアップサイトをクラウド上に構築するイメージ

モデルシステム 4 では、データのバックアップを同期で行い、待機サーバを「ホットスタンバイ」状態にしておく必要がある。この場合、メインサイトとバックアップサイト間で一定の伝送路容量を確保したり、専用の待機サーバを確保したりすることが必要となる可能性が高い。したがって、コストだけを考えると、現時点ではモデルシステム4の高回復力システム基盤についてクラウドサービスを利用することのメリットは少ないかもしれない。

Copyright © 2012 IPA, All Rights Reserved

4.2. 高回復力システム基盤の観点におけるクラウドサービス利用の留意点

4.2.1. クラウドサービス全般における留意点

(1)高回復力システム基盤の要件を満たす機能を提供するクラウドサービスは多彩である。また、サービスメニューや名称が同じようであっても、事業者ごとで機能、サービスレベルや利用技術などが異なる場合もある。クラウドサービスの選択時にはその内容をよく確かめる必要がある。

(2)市販ソフトウェアなどの中には、稼働するサーバのプロセッサ分のライセンス購入を必要とするものがある。(IP アドレス数でライセンスされるものなどもある。)このような場合、使用する可能性のあるクラウドサービスの全プロセッサのソフトウェアライセンス費用が発生し高額になってしまうこともあるので、ソフトウェアの価格体系などを確認する必要がある。

(3)クラウドサービスの利用を開始する前に、サービスの信頼性についてサーバ冗長化やバックアップサイトなどの対策を確認すべきである。サービスの稼働率、障害時の回復目標時間などのより具体的な情報については、SLA などの文書により確認すべきである。

(4)ネットワークサービスが使えないと、結果的にクラウドサービスも使えないため、ネットワークサービスの冗長化について検討すべきである。

(5)万が一クラウドサービスが停止した場合、利用者は自分でシステムを復旧することができない。このため、サービス停止のリスク(業務への影響度や発生確率など)を考慮し、対応策(代替手段)を検討しておくべきである。代替手段には、手作業による対応、他サービスへの切り替え、同じ業者の提供する代替サービスなどがある。

(6)大規模災害時等には、ユーザが大幅に増え、クラウドサービスのサービスレベルが低下することも起こり得る。クラウドサービスの信頼性の確認に加え、大規模災害時にクラウド事業者が、十分なリソースを提供できるかを見極める必要がある。

以上の点も含め、クラウドサービスを利用するにあたっては、サービスの機能・コスト・セキュリティなどについて事前に検討した上で利用しなければならない。クラウドサービス全般に関する注意事項などについては、以下のような資料が参考になる。

・IPA「中小企業のためのクラウドサービス安全利用の手引き」(2011 年 4 月)
(掲載 URL　http://www.ipa.go.jp/security/cloud/documents/cloud_tebiki_V1.pdf　)
・経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」(2011 年 4 月)
(掲載 URL　http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html　)
・特定非営利活動法人　ASP・SaaS・クラウドコンソーシアム(ASPIC)「クラウドサービス利用者の保護とコンプライアンス確保のためのガイド」(2011 年 7 月)
(掲載 URL　http://www.aspicjapan.org/information/publish/guide_ptotect/pdf/jp_ver1.pdf　)

Copyright © 2012 IPA, All Rights Reserved

4.2.2. データバックアップにクラウドサービスを利用する際の留意点

(1)データ転送量で課金が行われるクラウドサービスを利用する場合、バックアップデータの転送量が大きくなるとコスト負担が増える可能性がある。また、通信速度が遅い場合は、バックアップに時間がかかり、1日分のバックアップに 1 日以上かかるといったことも起こり得る。バックアップサービス利用時には、データ量・頻度を見定めて、ネットワークの帯域を確保する必要がある。

(2)クラウドサービスの利用料だけでなくネットワーク利用料も含めて運用コストについては、導入前に十分なシミュレーションを実施する必要がある。特に従量制による課金の場合はコストが大きく変動することがある。

(3)データ量が業績や業務内容の変動等により増加する場合や情報システムを更改する場合などでは、バックアップデータの転送量が大きくなりコスト負担が当初計画通りでなくなる可能性がある。導入時点ばかりでなく、将来のバックアップデータ量予測とコスト負担などへの対応についても同様に考慮しておく必要がある。

4.2.3. バックアップサイト構築にクラウドサービスを利用する際の留意点

(1)クラウドサービスを利用し、バックアップサイトを構築するためには、メインサイトで動作するアプリケーションソフトウェアがクラウド上で動作しなければならない。そのためには、クラウド上の OS でメインサイトのアプリケーション、DBMS 等のミドルウェアおよびパケージソフトウェアも、クラウドサービスの提供する環境で動作保障される必要がある。また、メインサイトでプライベートアドレスを利用している場合は、クラウドサービスにおいて、プライベートアドレスが利用できるものであることが望まれる。メインサイトのミドルウェア、アプリケーション、パッケージソフトなどが、クラウド上の仮想環境で動作することを確認する必要がある。

(2)メインサイトで動作している自社開発アプリケーションやパッケージソフトウェアのカスタマイズ部が、上記クラウドサービスの提供する環境での動作実績がない場合、クラウド上での動作確認試験を実施することが望ましい。

(3)障害発生時の切り替え手順や、再度メインサイトでの運用 状態に戻す手順については、導入前に検討する必要がある。クラウドサービスの場合、管理者権限などが制限されたり、利用できるソフトウェアが制限されたりするからである。以下のような点をクラウド事業者に確認しておく必要がある。

・切り替え手順
・事業者の対応可能時間帯や切り替え所要時間
・切り替え後の運用について、クラウドサービスの OS などへのアクセス権
・切戻し(再度メインサイトでの運用状態に戻す手順)についてのデータ転送などの条件
・訓練の実施内容や方法

Copyright © 2012 IPA, All Rights Reserved

5. 付録　高回復力システム基盤の要件と各事例との対比表

Copyright © 2012 IPA, All Rights Reserved