情報システム基盤の復旧に関する
対策の調査
報告書

2012 年 7 月

独立行政法人情報処理推進機構

はじめに

独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター（以下「IPA/SEC」とします。）では、企業等における情報システム基盤の復旧能力の向上を図り、ひいては社会のレジリエンスを全体的に底上げすることを目的に、東日本大震災発生前後の企業における情報システムの復旧対策や意識の変化、復旧にあたり有益と考えられる仮想化やクラウド等の新しい技術やサービス、企業等におけるデータの保管対象や方法、復旧対策の事例等について調査を実施し、その結果を調査報告書としてとりまとめました。

本調査研究は、「情報システム基盤の復旧に関する対策の調査」として、株式会社情報通信総合研究所に委託し、実施しました。

情報システム基盤の復旧に関する対策の調査
【調査報告書】

独立行政法人情報処理推進機構

目　次

1　調査の目的および調査の方法

1.1 調査の背景と目的

1.1.1 背景

2011 年 3 月 11 日に発生した東日本大震災の影響で、従来の「想定」を大きく超える事象が輻輳的に生じたが、情報システム基盤の復旧には仮想化技術やクラウド等新たな技術やサービスの利用による成果が報告された。その反面、管理の枠組みを導入する際に必要なリスク分析等の手順が複雑なため、必要性は理解しているが具体的対策の着手には至っていない企業が多いことが課題として挙げられている。同様に、事前に想定したリスクに基づき対応手順等を用意するため、「想定外」の事態に柔軟に対応できない場合が多かったことも課題として指摘されている。

IPA/SEC では、経済産業省が 2003 年に策定した「情報セキュリティ総合戦略」の「しなやかな「事故前提社会システム」の構築（高回復力・被害局限化の確保）」という基本方針に改めて着目し、従来のマネジメントシステムという組織管理の手法にレジリエンス (Resilience：弾力、回復力)という視点から、企業等が取り組むべき方向性について調査研究を行うこととなった。

1.1.2 目的

本調査研究においては、東日本大震災発生前後の企業における情報システムの復旧対策や意識の変化、復旧にあたり有益と考えられる仮想化やクラウド等の新しい技術やサービス、企業等におけるデータの保管対象や方法、復旧対策の事例等を調査し、報告書として取りまとめる。

これにより、事業継続計画の策定や情報システムの継続的な利用をより広く普及し、より平易な内容でその指針を提供することで、企業等における情報システム基盤の復旧能力の向上を図り、ひいては社会のレジリエンスを全体的に底上げに資することを目的とする。

1.2 調査の対象範囲

本調査の対象範囲は、企業等の IT サービス継続マネジメントと情報システム基盤に対する復旧対策をおもな対象範囲とする。ここでいう情報システム基盤とは、「電源供給・ネットワークサービス」（以下、「通信・電力」とする）、「建物設備」、「ハードウェア機器やネットワーク機器」、「OS やミドルウェア」、「システム運用の体制や仕組み」、「ハードディスク等に格納された業務アプリケーション・業務データ（以下、「業務アプリケーション・業務データ」とする）」を指す（IPA/SEC「高回復力システム基盤導入ガイド　概要編」（2012 年 5 月）における表 2.1-1「高回復力システム基盤導入の基本的な考え方」における「構成要素」による）。

1.3 調査の方法と項目

本調査は、対象範囲の調査を広く行うため、文献調査、アンケート調査、ヒアリング調査を行った。それらの調査結果をもとに、考察を行った。具体的には、以下のとおり実施した。

1.3.1 文献調査

報告書や専門書籍、雑誌、Web 掲載資料等の文献資料を対象に、以下の事項について調査を実施した。

①被災前後における企業の対策状況と意識の変化、東日本大震災における情報システム基盤の被災状況や復旧対応
②システム復旧に関連する新しい技術やサービス
③情報システム基盤の復旧に関する対策に資する国際規格やガイドライン

1.3.2 アンケート調査

上場企業および非上場の資本金 1 億円以上の企業のうち、信用調査会社が保有するデータベースの中から任意に抽出した 3,000 社を対象に、以下の事項について調査を実施した。

①IT サービス継続に対する意識や平常時の準備や活動
②コンピュータシステムと新しい技術の採用状況
③システム構成
④リカバリ要件定義の有無
⑤データの保管（バックアップ）の実施状況
⑥震災被害やその他の障害の経験とその後の対応

1.3.3 ヒアリング調査

上記のアンケート調査の回答企業を中心に、システム復旧対策を実施している企業や地方公共団体 11 団体を対象に、以下の事項について調査を実施した。

①事業の特徴と IT
②重要業務と継続戦略
③重要業務のためのシステム基盤の概要
④システム復旧対策のポイントと留意点
⑤システム復旧対策の詳細

1.3.4 考察

調査結果をもとに、企業等における情報システム基盤の復旧能力の向上を図るための取り組みの考え方について考察する。

1.4 調査の注視点

情報システム基盤の回復力を高めていくためには、具体的にどのような対策があり、また有効であるかを知り、実行していくことが重要である。その際、先の東日本大震災の経験を踏まえ、どのような対策が重要であるかを調査することが有益である。

また、同じ対策がどの企業にとっても有効であるとは限らない。経営資源の制約があるため、高度な対策を自由に実施できる企業は限られる。復旧対策を、企業経営の中でどのように組み込み、マネジメントしていくことが有効か、という観点も重要である。

このような考えから、本調査では、企業における情報システム基盤の復旧能力を向上させるためには、東日本大震災の経験を生かすことに留意しながら、「IT サービス継続マネジメントの観点」と「技術的対策等の観点」の 2 つの観点に注視して、企業等の情報システム基盤の復旧対策について調査することが重要であると考えた。具体的には、図 1-1 に示すような観点に注視して、調査した。

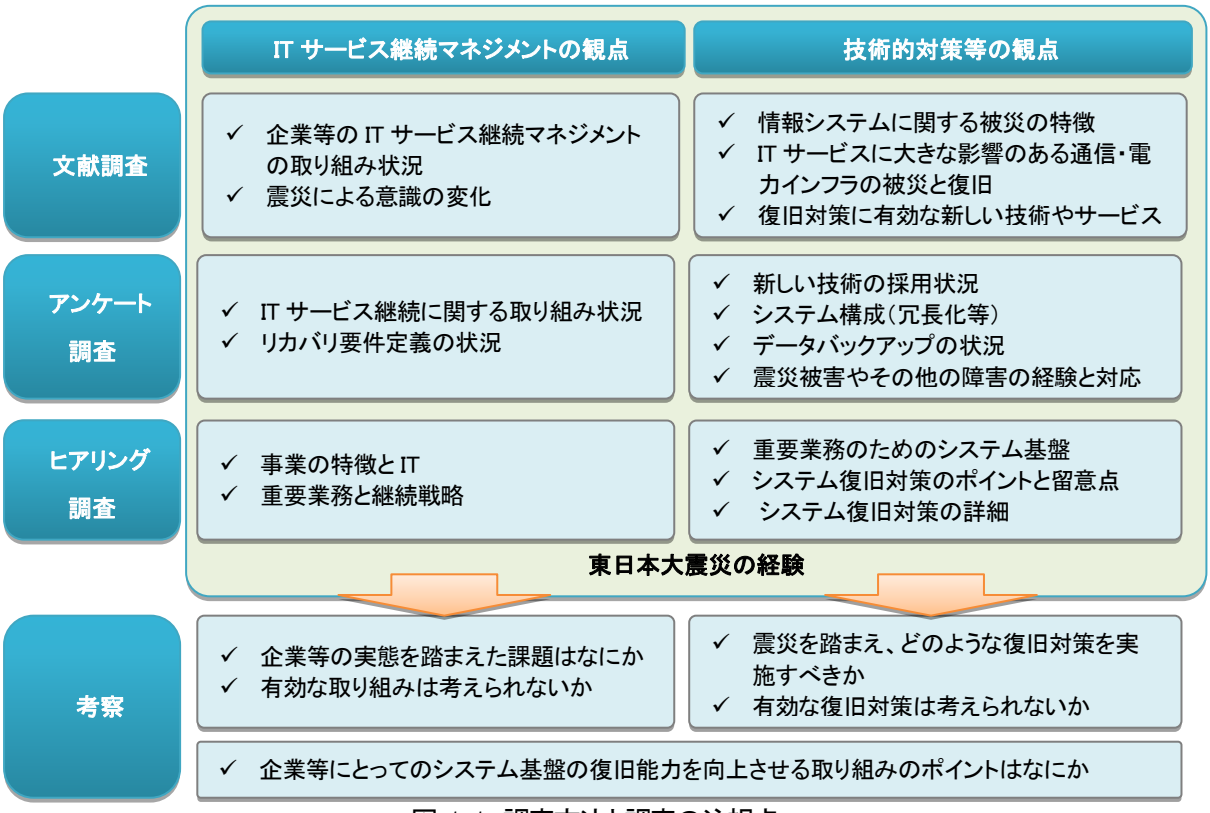


図 1-1 調査方法と調査の注視点

2　東日本大震災による IT への影響と対策の動向

2.1 企業等における動向

2.1.1 調査の概要と前提

(1) 調査の概要

東日本大震災では、被災地を中心に情報システムにも大きな被害が生じた。直接被災がなかった企業等の意識にも影響を与えた。ここでは、企業の IT サービス継続の取り組みや意識の変化等について、文献調査を実施した。調査の概要は表 2-1 に示すとおりである。

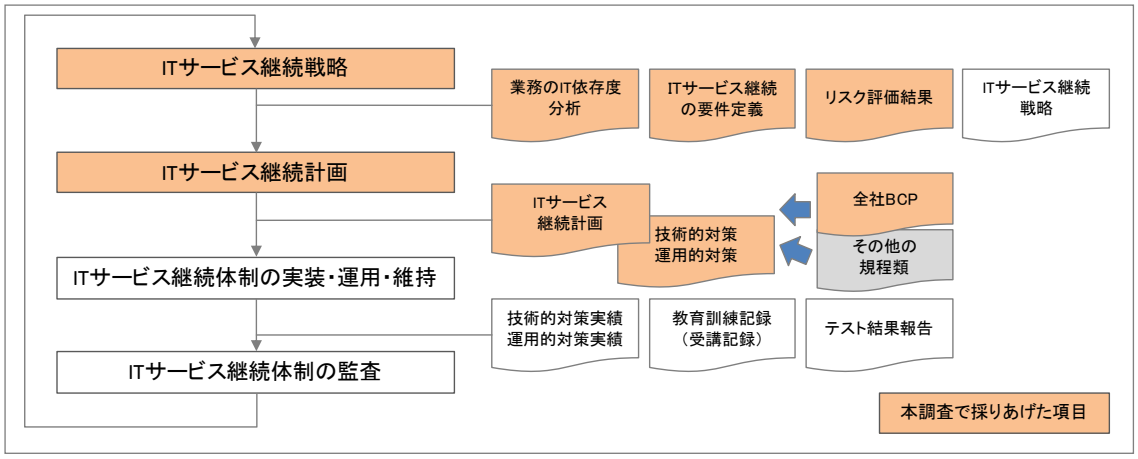
表 2-1　文献調査(企業等における動向)の概要

項目	内容
調査目的	東日本大震災前後の企業における IT サービス継続の取り組みの現状や変化を調査し、IT サービス継続における課題を探るため
調査対象	主に震災を受けて調査された事業継続やシステム復旧、災害対策に関する文献 ・国の報告書 ・各種団体、民間企業の報告書 ・専門書籍・雑誌　等
調査項目	・企業等の IT サービス継続の取り組み状況 ・企業等の震災による意識の変化 ・情報システム基盤の被災状況
調査時期	2012 年 3 月～4 月

(2) 調査の前提

ここでは、企業等の IT サービス継続の取り組みや意識の変化等について、IT サービス継続マネジメントの流れに沿ってまとめる。IT サービス継続は、事業継続(事業継続計画(以下、「BCP」とする。)及び事業継続マネジメント(以下、「BCM」とする。))、リスクマネジメントとも密接な関係がある。巻末の「付録②　情報システム基盤の復旧に関する対策に資する国際規格やガイドライン」に、事業継続、IT サービス継続、リスクマネジメントに関する国際規格やガイドラインを整理した。本調査では、これらの国際規格やガイドラインの考え方が反映されていると考えられる経済産業省「IT サービス継続ガイドライン」(2008 年 9 月)(掲載 URL:http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf)を参照する。

具体的には、「IT サービス継続ガイドライン」に示された代表的な項目(図 2-1)に沿って、各項目で実施するプロセスに関係する企業の取り組みや意識等について調査した。



出所：経済産業省「IT サービス継続ガイドライン」（2008 年 9 月）をもとに作成

図 2-1 「IT サービス継続ガイドライン」におけるマネジメントのフレームワークと文献調査の整理項目

2.1.2 企業等の IT サービス継続戦略に関する認識の変化

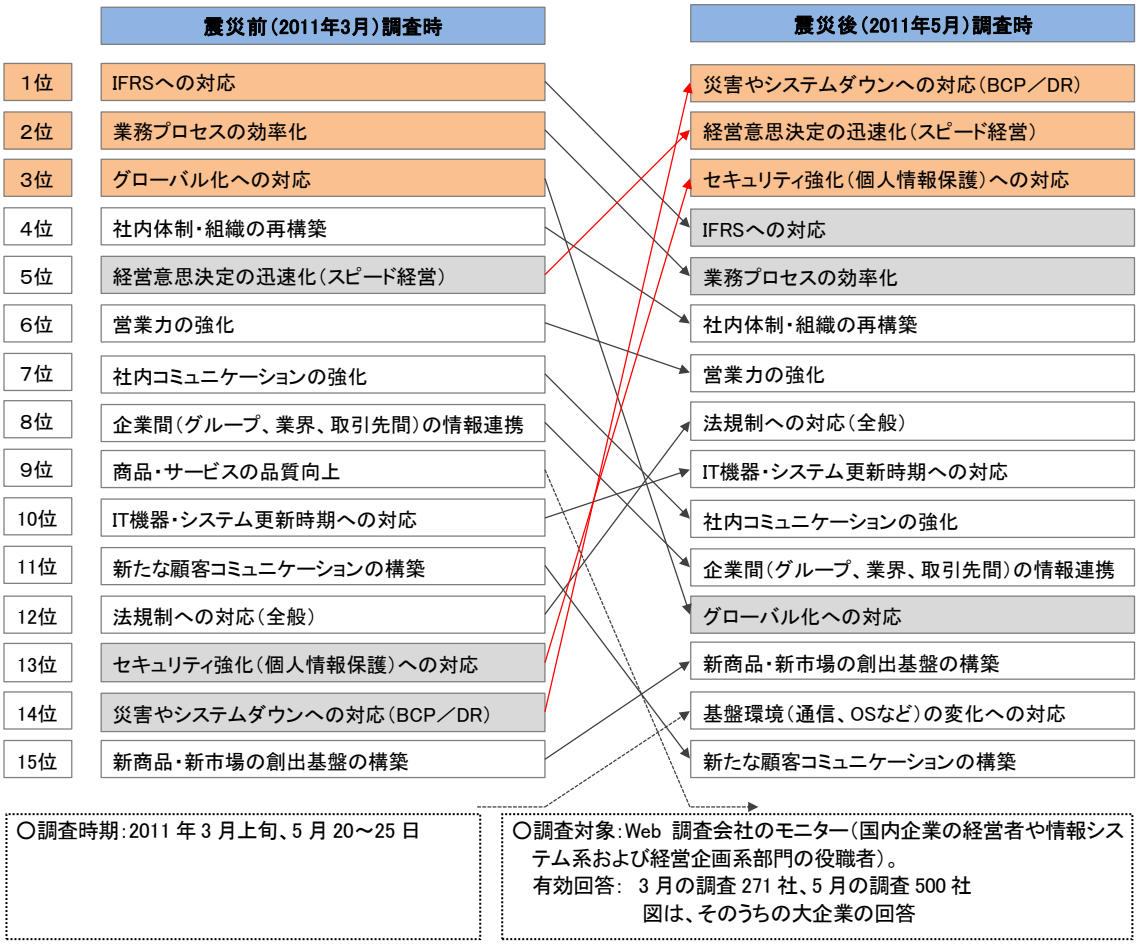
(1) 業務の IT 依存度分析

① 重視する経営課題の変化

「IT サービス継続ガイドライン」では、「業務の IT 依存度の分析」を行う旨を示している。ここでは、企業の「業務の IT 依存度」への認識を示す資料として、IT に関する災害対策への認識についての調査結果を示す。

日本情報経済社会推進協会（JIPDEC）の調査によると、今後 1～3 年間で重視する経営課題について、大企業からの回答を比較すると、図 2-2 に示すように、「災害やシステムダウンへの対応（BCP/DR（ディザスタリカバリ））」が震災前 14 位であったのが、震災後には第 1 位と順位を大きく上げている。第 2 位の「経営意思決定の迅速化（スピード経営）」、第 3 位の「セキュリティ強化（個人情報保護）への対応」も前年度から順位を上げている。

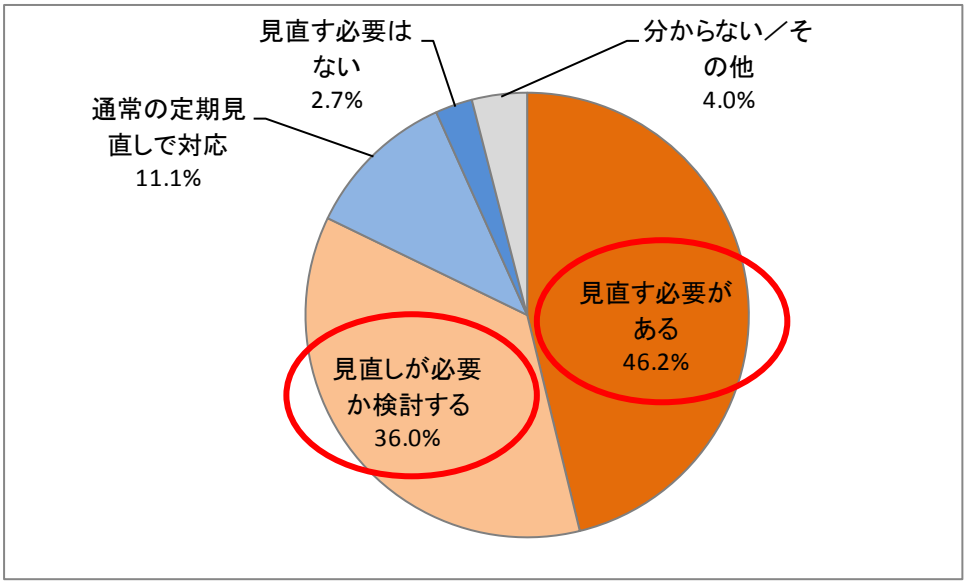
「災害やシステムダウンへの対応（BCP/DR）」が第 1 位として挙げられていることから、東日本大震災を受けて、企業において IT の側面を含む災害対策がきわめて重要な経営課題と認識されていることが分かる。



本調査は、当初 3 月上旬に実施されたが震災を受け一旦中断し、5 月に再調査を実施
上記は、この 3 月時点の調査結果と 5 月時点の調査結果を比較したもの
出所:一般財団法人日本情報経済社会推進協会「企業 IT 利活用動向調査」(2011 年 11 月)

図 2-2 震災前後の今後 1～3 年で重視する経営課題(大企業) (震災前 n=88、震災後 n=172)

また、日経 BP 社の調査によると、図 2-3 に示すとおり、震災後、システム環境の災害対策を「見直す必要がある」(46.2%)、「見直しが必要か検討する」(36.0%)と回答している企業があわせて 82.2%に上っている。



〇調査時期:2011 年 3 月 30 日～4 月 5 日　〇調査対象:『日経コミュニケーション』誌読者モニター225 社

出所:日経 BP 社『IT で実現する震災・省電力 BCP 完全ガイド』(2011 年 7 月)(初出:『日経コミュニケーション』2011 年 5 月号)

図 2-3　東日本大震災を受けてシステム環境の災害対策を見直す必要性(n=225)

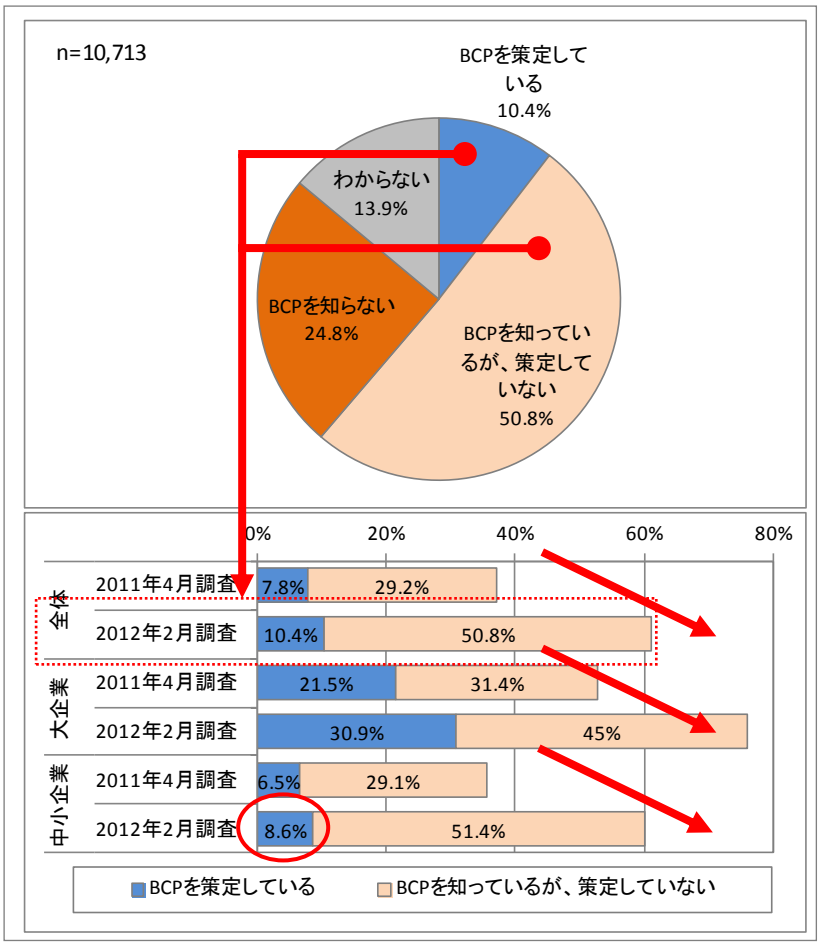
以上の調査結果から、企業では、東日本大震災を受け、IT に対する災害対策が重要であることについて、認識が深まっている様子がうかがえる。

② BCP(事業継続計画)の策定状況

「IT サービス継続ガイドライン」では、「業務の IT 依存度」の分析に際しての BCP の活用について示している。具体的には、BCP が策定され、維持すべき業務の明確化やビジネスインパクト分析(BIA)が実施されている場合には、これらを業務の IT 依存度の分析に活用することを解説している。ここでは関連する取り組みとして、東日本大震災前後の企業の BCP 策定状況について取り上げた。

帝国データバンクが実施した企業の BCP について調査した結果によると、図 2-4 の上段に示すように「BCP を策定している」と回答のあった企業は 10.4%であり、「BCP を知っているが、策定していない」と回答のあった企業は 50.8%であった。BCP を認知している企業は 6 割を超えるが、実際に策定している企業は少ないことが分かる。

また震災直後の 2011 年 4 月と 2012 年 2 月の時点の調査結果を比較すると、図 2-4 の下段に示すように BCP の認知率は全体で 37.0%(7.8%＋29.2%)から 61.2%(10.4%＋50.8%)まで増え、認知が進んでいることが分かる。しかし、実際に策定している企業は増えていない。とくに中小企業においては、6.5%から 8.6%と比率としては伸びているものの、策定済みの企業はまだ少数であることが分かる。



〇調査時期：2011 年 4 月
2012 年 2 月

〇調査対象：
・2011 年 4 月調査：TDB 景気動向調査登録企業 22,240 社、回答 10,769 社）
・2012 年 2 月調査：TDB 景気動向調査登録企業 23,651 社、回答 10,713 社

出所：帝国データバンク「BCP(事業継続計画)についての企業の意識調査」(2012 年 3 月)より作成
（掲載 URL：http://www.tdb.co.jp/report/watching/press/p120308.html）

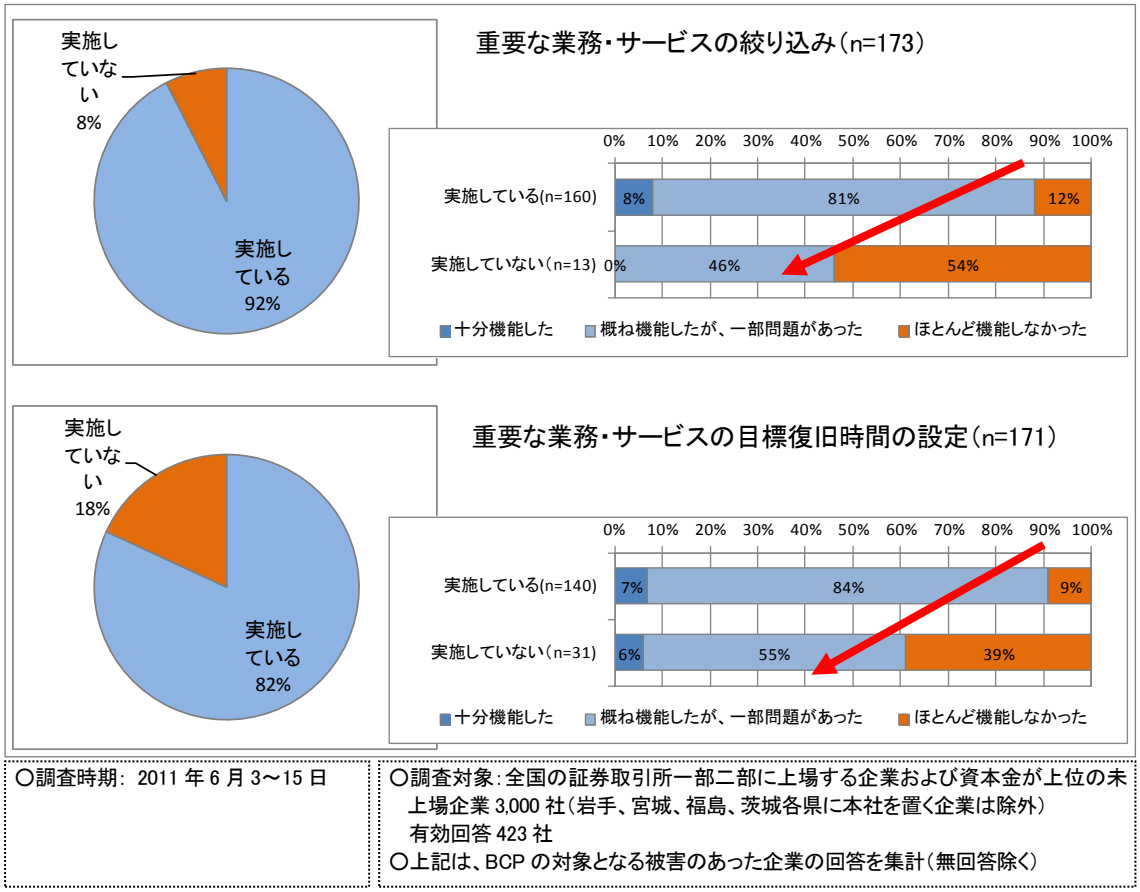
図 2-4 BCP の策定状況

(2) IT サービス継続の要件定義

「IT サービス継続ガイドライン」では、IT サービスの要件定義として、IT サービス継続マネジメントの範囲と IT サービスについての復旧目標(目標復旧時間(RTO)等)を定める旨が示されている。これに関連する資料として、文献調査からは、IT サービス継続に関する調査結果は得られなかった。ここでは、文献調査で得られた IT に限定しない BCP 全般について、企業等の目標設定等の実施状況について取り上げる。

① 要件定義の実施状況

野村総合研究所の BCP に関する調査結果によると、図 2-5 に示すように BCP を策定している企業のうち、「重要な業務・サービスの絞り込み」を実施している企業は 92%、「重要な業務・サービスの目標復旧時間」を設定している企業は 82%であり、多くの企業がこの 2 つを実施していることが分かる。この 2 つについて、「実施している」企業と「実施していない」企業の BCP の評価については、いずれの場合も、「実施していない」企業では、「BCP がほとんど機能しなかった」という企業の割合が増える傾向にある。この 2 つは、BCP において実施しておくことの重要性が高い事項と考える。



○調査時期: 2011 年 6 月 3～15 日

○調査対象:全国の証券取引所一部二部に上場する企業および資本金が上位の未上場企業 3,000 社(岩手、宮城、福島、茨城各県に本社を置く企業は除外)
有効回答 423 社
○上記は、BCP の対象となる被害のあった企業の回答を集計(無回答除く)

出所:野村総合研究所の 2012 年 6 月 30 日付ニュースリリース「大手企業の 26%で重要業務の停止が発生～東日本大震災の影響と BCP(事業継続計画)に関するアンケート調査結果～」図 7 より作成
(掲載 URL:http://www.nri.co.jp/news/2011/110630_1.html)

図 2-5 BCP の検討項目の実施状況と自社の BCP の評価

(3) リスク評価

「IT サービス継続ガイドライン」では、IT サービスを支える情報システムに対するリスクの評価について示している。ここでは、リスク評価に関連して、まず東日本大震災が、情報システムに対してどのような被害をもたらしたかを示し、次に東日本大震災以降、企業がどのようなリスクを想定しているかについて示す。

① 被災状況

東日本大震災では、IT に関して、表 2-2 に示すような被害をもたらした。

特徴的であったのは、津波によるサーバ等機器の水没や流失、広域的な被害、原子力災害によるシステムの運用困難と影響の長期化であった。また、通信、電力の停止が長期化、広域化したことが特徴であった。これらの被害は、今まで経験したことのない被害であった。なお、通信や電力についての被災と復旧については、「2.2 IT サービスに関連する社会インフラの被災と復旧」に詳しく示す。

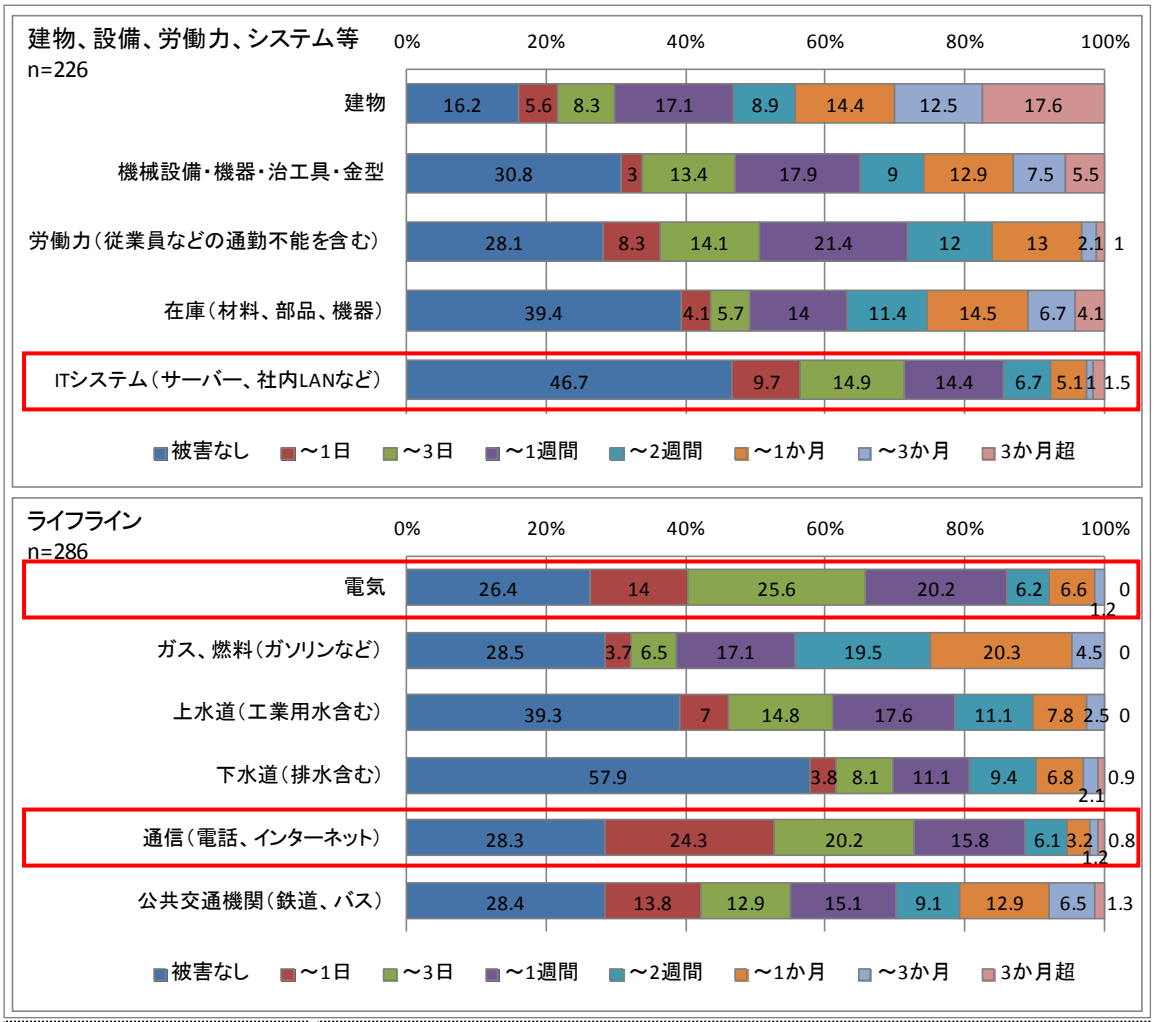
表 2-2 東日本大震災における IT に関するおもな被害

大項目	被害・影響	事例
地震動	サーバや PC 等の機器の損壊	・岩手県、宮城県、福島県等の広い範囲の企業等で建物や機器等が損傷。 ・例：福島県国見町では倒壊のおそれから庁舎での運用が不可能になり、他の公共施設に移設して運用。その後 SaaS 利用に移行。
津波	サーバや PC 等機器の水没や流出	・岩手県、宮城県、福島県沿岸の企業や地方公共団体で機器が水没、流出。 ・例：陸前高田市では、庁舎が津波浸水しサーバが水没。ハードディスクのデータの復旧作業や外部保管データ等を活用して復旧。
原子力災害	立ち入り禁止区域内に設置してある情報システムの運用が困難	・福島第一原子力発電所周辺の警戒区域や緊急時避難準備区域、計画的避難区域に立地する企業等でシステム運用が困難化。
停電	停電によるシステムの停止	・東北電力、東京電力管内の企業等で、システムが停止。 ・例：東北地方の多数の銀行の被災事業所の ATM が利用不能。 ・停電の長期化とともに燃料の供給も困難になったため、自家用発電機が運用困難となる例があった。
	計画停電によるシステムの運用停止	・計画停電区域内にある企業等でシステムを一時停止。 ・例：情報提供サービスやゲーム等のオンラインサービス、地方公共団体の窓口サービスが一時運用停止。
通信遮断	ネットワークの停止	・東北地方を中心とする企業等で、オンラインシステム等が利用不能。 ・例：石巻市では、沿岸部で津波により光ファイバ網等が被災。通信確保に衛星通信回線等を活用。

出所：東日本大震災被災地自治体 ICT 連絡会（ISN）「東日本大震災と自治体 ICT 公開セミナー」資料（平成 23 年 11 月）（掲載 URL: http://www.city.sendai.jp/shisei/1201134_1984.html）ほか、各種公表資料より作成。

また、東京海上日動リスクコンサルティングが実施した被災地の企業を対象とした調査では、図 2-6 上段に示すように、東日本大震災の被害に対する復旧期間について調査している。これによると、「IT システム」については、半数以上の企業で被害が発生しており、被害がなかった企業も含め 9 割以上の企業で復旧するまでに 2 週間を要している。

また、ライフラインについては、図 2-6 下段に示すように、システムに関連の深い「電気」、「通信」とも 7 割以上の企業で被害が発生し、被害がなかった企業も含め 9 割以上の企業で復旧するまでに 2 週間を要している。



○調査時期：2011 年 9 月

○調査対象：岩手県、宮城県、福島県、茨城県、栃木県に所在する企業 1000 社
（大企業では本社もしくは事業所が所在、中堅・中小企業においては本社が所在）
○有効回答：286 社（大企業製造業 49 社、大企業非製造業 56 社、中堅企業製造業 48 社、中堅企業非製造業 74 社、中小企業 59 社）

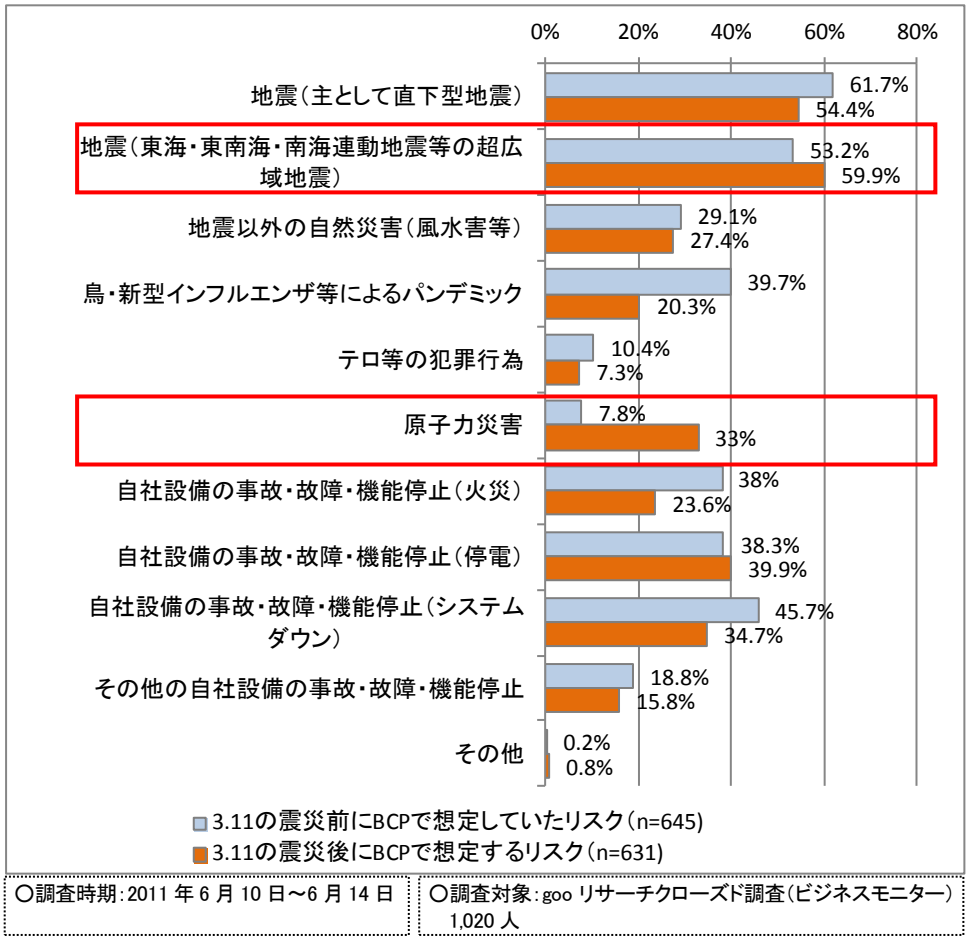
出所：東京海上日動リスクコンサルティング株式会社「東日本大震災と事業継続計画（BCP）に関するアンケート調査」『TALISMAN』2011 年 12 月号

図 2-6 被害を受けた項目別の復旧期間

② 全般的なリスクの認識

ここでは、東日本大震災を受けて、企業がどのようなリスクを想定しているかについての調査結果を示す。

NTT データ経営研究所の東日本大震災を受けた企業の事業継続に係る意識調査によると、自社の BCP を見直す（新たに BCP を策定する）企業について、図 2-7 に示すように、震災前は「地震（主として直下型地震）」を想定する企業が多かったが、震災後は「地震（東海・東南海・南海連動地震等の超広域地震）」を想定する企業が 59.9%ともっとも多い。また、特に「原子力災害」を挙げる企業が、震災前後で 7.8%から 33%と大きく増えている。なお、調査を実施した 2011 年 6 月は、原子力災害についての報道等でも大きく取り上げられていた時期でもあり、とくに注目を集めていた可能性がある。



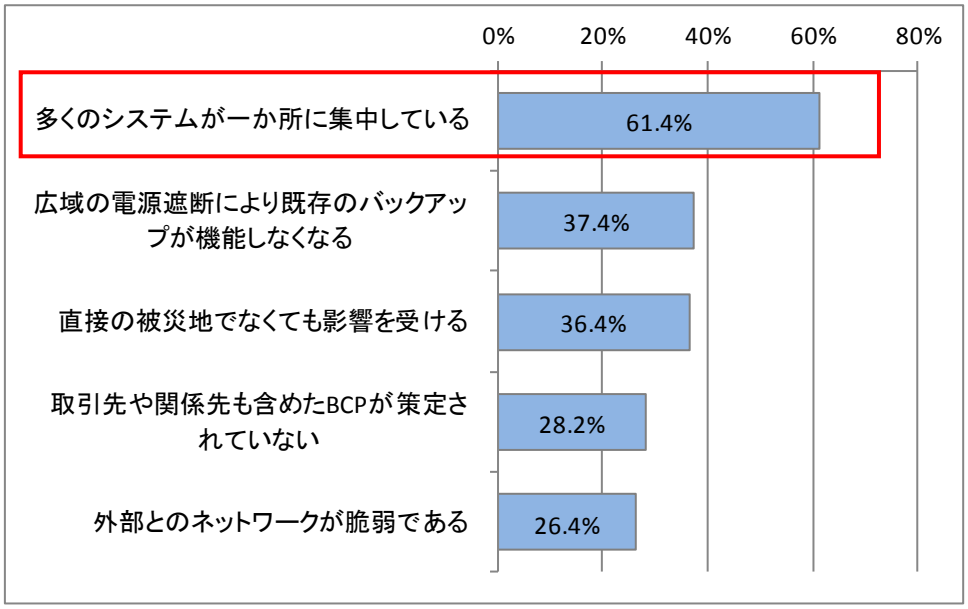
出所：「東日本大震災を受けた企業の事業継続に係る意識調査」（2011 年 7 月）NTT データ経営研究所 / goo リサーチ（NTT レゾナント）
（掲載 URL: http://www.keieiken.co.jp/aboutus/newsrelease/110719/）

図 2-7 3.11 の震災をうけた BCP 見直し・策定において想定するリスク（震災前との比較）

③ IT に対するリスクの認識

ここでは、東日本大震災を受けて、企業が IT についてどのようなリスクを想定しているかについての調査結果を示す。

日本情報システム・ユーザー協会（JUAS）による IT 部門として対策が必要なリスクについての調査結果を図 2-8 に示す。これによると、「多くのシステムが一か所に集中している」ことが、IT 部門で対策が必要とされるリスクの第一位となっている。企業においては、大規模災害時の対策として、システムの分散配置が課題となっているものと考えられる。



出所：日本情報システム・ユーザー協会「企業 IT 動向調査 2012」（2012 年 3 月）

図 2-8 東日本大震災を機に認識した、IT 部門で対策が必要とされるリスク（n=922）

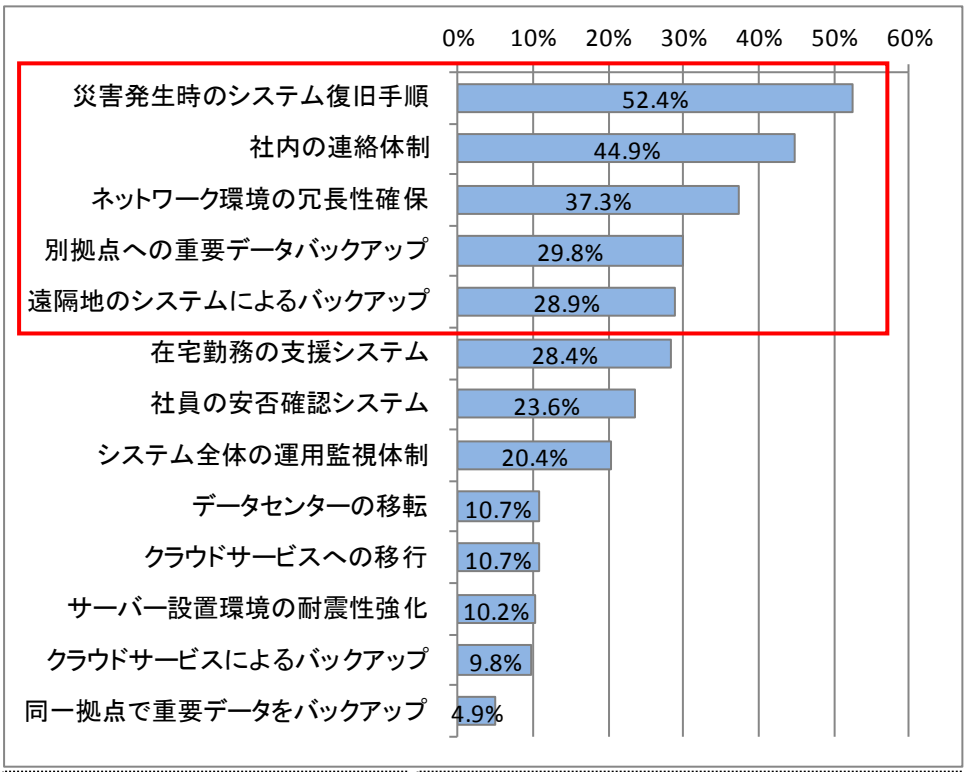
2.1.3　企業等の IT サービス継続に向けた計画と対策の状況変化

(1) 対策実施計画

「IT サービス継続ガイドライン」では、IT サービス継続戦略を実現するための具体的な対策内容を対策実施計画として決定する旨を示している。ここでは、これに関連する資料として、企業の具体的な復旧対策の実施に関する意識について示す。

① 対策全般についての意向

日経 BP 社の調査によると、東日本大震災後、企業では、システム環境の災害対策について、図 2-9 に示すような事項について見直したいとしている。すなわち、「災害発生時のシステム復旧手順」、「社内の連絡体制」といった運用面の対策に続き、「ネットワーク環境の冗長性確保」、「別拠点への重要データバックアップ」、「遠隔地のシステムによるバックアップ」等の対策が上位となっている。

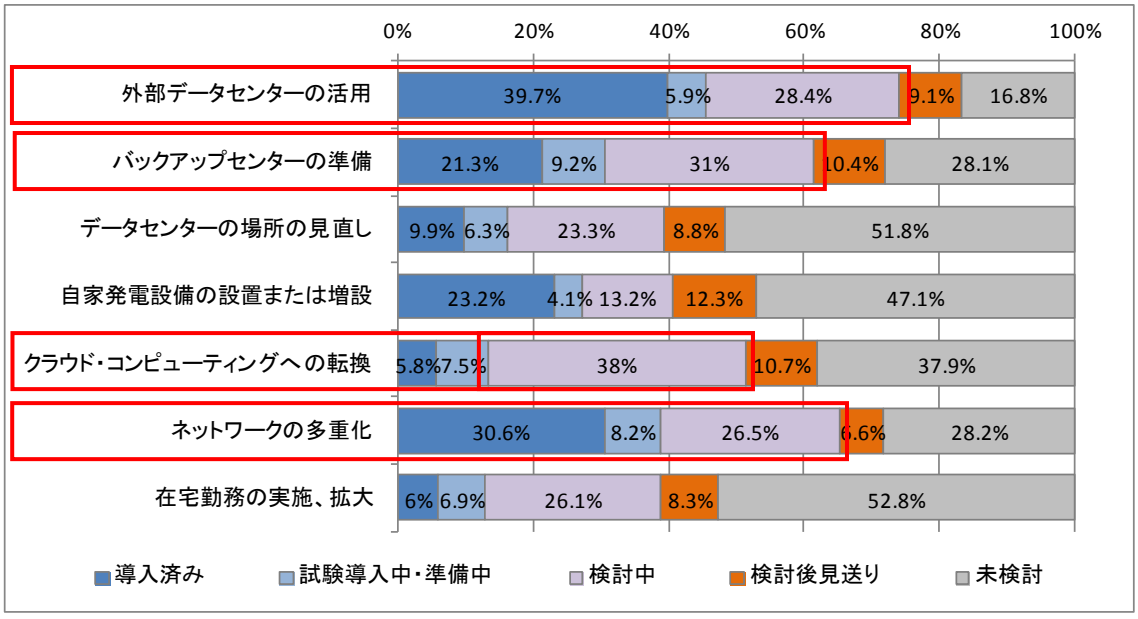


出所:日経 BP 社『IT で実現する震災・省電力 BCP 完全ガイド』(2011 年 7 月)(初出:『日経コミュニケーション』2011 年 5 月号)

図 2-9　システム環境の災害対策で見直したい点(n=225)

また、日本情報システム・ユーザー協会（JUAS）が実施した企業の IT 利用動向に関する調査によれば、IT 部門が BCP を策定または見直す場合のポイントについて調査した結果は図 2-10 のようになっている。

「導入済み」、「試験導入中・準備中」、「検討中」をあわせると、「外部データセンタの活用」、「ネットワークの多重化」、「バックアップセンターの準備」の順で多い。また「検討中」だけを見ると、「クラウド・コンピューティングへの転換」が多く、長期的にはクラウド活用が進む可能性がある。なお、先述の日経 BP 社の調査では、「クラウドサービスへの移行」、「クラウドサービスによるバックアップ」は見直したい点の上位にはなかった。これは、日経 BP 社の調査が震災後すぐに実施されたものであるのに対して JUAS 調査は、震災から約半年後に実施されたものであり、クラウドの災害対策への有効性が広く認識された結果である可能性がある。



○調査時期：2011 年 10 月 29 日～11 月 21 日

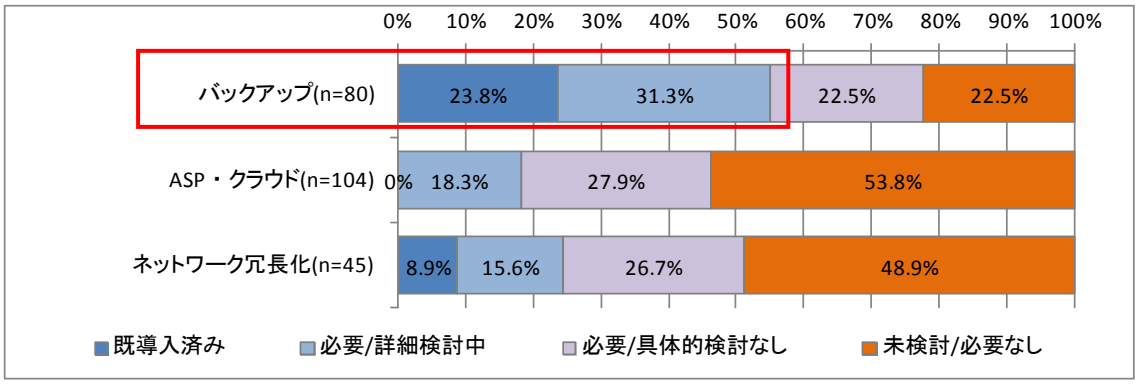
○調査対象：東証一部上場企業とそれに準ずる企業の計 4,000 社（各 IT 部門長宛送付）

出所：日本情報システム・ユーザー協会「企業 IT 動向調査 2012」（2012 年 3 月）
（掲載 URL：http://www.juas.or.jp/servey/it12/index.html）

図 2-10 BCP 策定・見直しのポイント（n=944）

② 被災地における意向

総務省が実施した、被災地の企業や自治体等を対象とした調査(図 2-11)で、今後の IT 環境に関するニーズについて、「バックアップ」、「ネットワーク冗長化」、「ASP・クラウド」の 3 つについての調査結果では、「バックアップ」（データバックアップ）がもっともニーズが高く、他の 2 つに比べて差があった。被災経験者は、なによりデータ保全対策が重要であると認識していることが分かる。



○調査時期:2011 年 9 月～2012 年 1 月

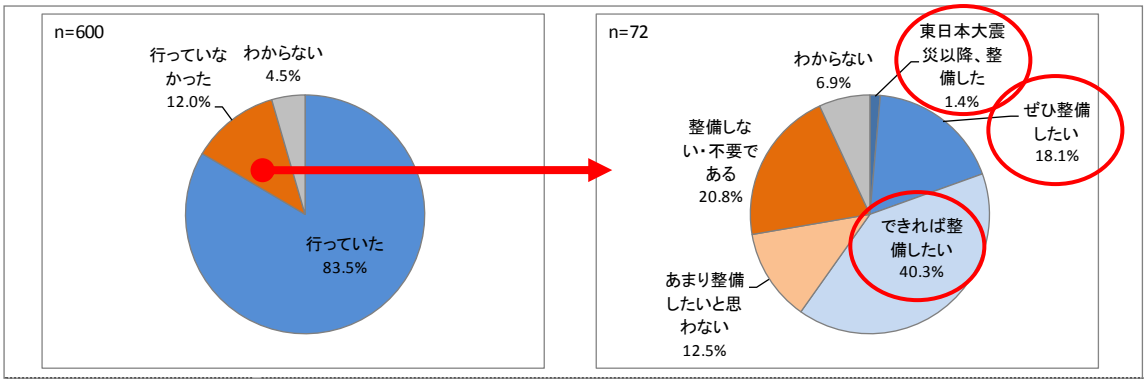
○調査対象:岩手県宮古市・ 大槌町・釜石市・大船渡市・陸前高田市、宮城県気仙沼市・南三陸町・石巻市・仙台市・名取市、福島県南相馬市・いわき市で被災された方・ボランティア等の活動をされている方:306 件

出所:総務省「災害時における情報通信の在り方に関する調査結果」(2012 年 3 月)
(掲載 URL: http://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000036.html)

図 2-11 今後の IT 環境に関するニーズ

③ データバックアップに関する意向

矢野経済研究所が実施した災害対策ソリューション市場に関する調査によると、図 2-12 に示すように、基幹システムについては、東日本大震災以前に 8 割以上の企業がデータバックアップを実施している。東日本大震災以降の状況をみると、行っていなかった企業についても「東日本大震災以降、整備した」、「ぜひ整備したい」、「できれば整備したい」をあわせて過半数の企業がバックアップを実施しているか、実施したいという意向を持っている。被災地に限らず、企業のデータバックアップの意向は強いことが分かる。



○調査時期:2011 年 5 月

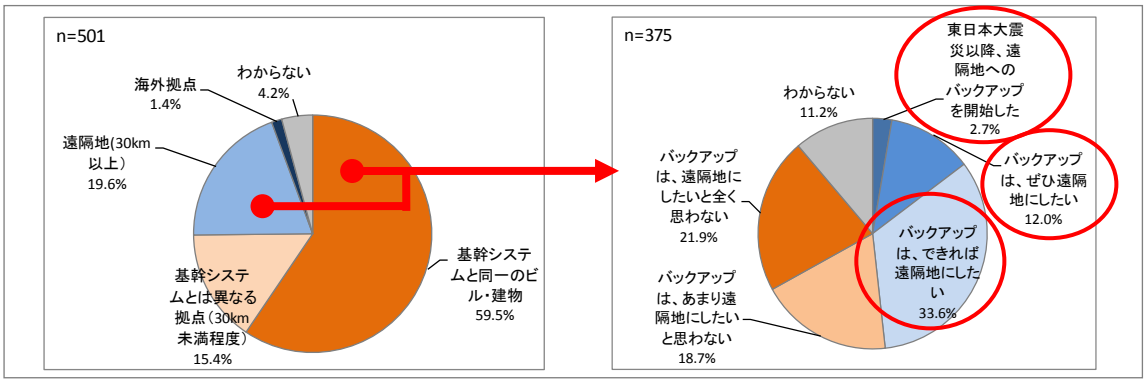
○調査対象(集計対象):売上高 1 億円以上の企業に勤務(もしくは経営し)、かつ社内情報システム全般について選定ないしは最終決裁を担当する 600 名、そのうち右図については左図で東日本大震災以前の基幹バックアップについて「行っていなかった」と回答した 72 名

○調査方法:インターネット形式、いずれも単数回答

出所:株式会社矢野経済研究所『東日本大震災後の災害対策ソリューション市場』(2011 年 6 月)

図 2-12 大震災以前の基幹システムのバックアップの実施状況と意欲の変化

また、基幹システムのバックアップデータの保管場所については、同じく矢野経済研究所が実施した調査によると、図 2-13 に示すように大震災以前の時点で約 6 割の企業が「基幹システムと同一のビル・建物」となっている。また、同調査で「基幹システムと同一のビル・建物」、「基幹システムとは異なる拠点（30km 未満程度）」と回答のあった企業について、約半数が東日本大震災以降、遠隔地バックアップの実施を開始したか、遠隔地バックアップを実施したいという意向を持っている。



〇調査時期：2011 年 5 月

〇調査対象（集計対象）：売上高 1 億円以上の企業に勤務（もしくは経営し）、かつ社内情報システム全般について選定ないしは最終決裁を担当する 600 名、そのうち左図については東日本大震災以前の基幹バックアップについて「行っていた」と回答した 501 名、右図については左図で基幹バックアップを「同一のビル・建物」および「異なる拠点（30km 未満程度）」と回答した 375 名
〇調査方法：インターネット形式、いずれも単数回答

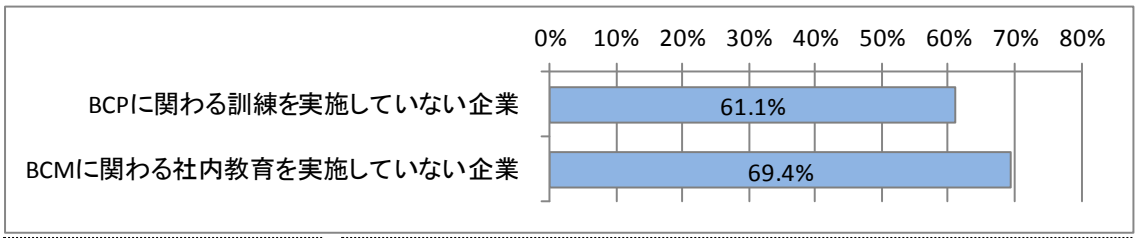
出所：株式会社矢野経済研究所『東日本大震災後の災害対策ソリューション市場』(2011 年 6 月)

図 2-13 大震災以前の基幹システムの遠隔地バックアップの実施状況と意欲の変化

(2) 教育訓練計画

「IT サービス継続ガイドライン」では、IT サービス継続計画を組織内に定着化し、緊急時の対応能力を高めていくための教育訓練計画を策定する旨を示している。これに関連して、文献調査からは、IT サービス継続に限定した教育訓練についての調査結果は得られなかった。ここでは、IT に限定しない企業の BCP 全般についての教育訓練の実施状況について示す。

インターリスク総研の事業継続マネジメントに関する調査によれば、図 2-14 に示すように、「BCP に関わる訓練を実施していない企業」は 61.1%、「BCM に関わる社内教育を実施していない企業」は、69.4%を占めている。本調査は上場企業を対象としており、上場しているような大企業でも教育訓練は十分に実施されていない様子がうかがえる。



〇調査時期：2011 年 8 月～9 月
〇調査対象：日本の全上場企業 3,209 社（ただし被災地に本社を置く企業は除く）

出所：インターリスク総研「第 5 回事業継続マネジメントに関する日本企業の実態調査」「東日本大震災から 1 年」（2012 年 3 月）より作成

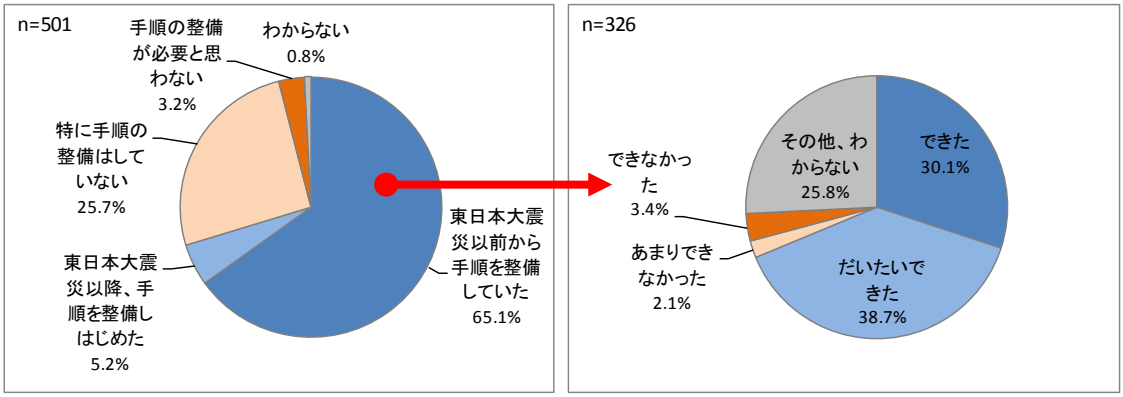
図 2-14 BCP 策定後の取り組み

(3) 事後対応計画(緊急時対応計画)

「IT サービス継続ガイドライン」では、緊急事態が発生した際に、情報システムを迅速に復旧し再開するために、必要な体制や対応方法を定めた事後対応計画の策定する旨を示している。ここでは、関連する内容として、バックアップからの復旧手順についての調査結果を示す。

矢野経済研究所が実施した災害対策ソリューション市場に関する調査によれば、図 2-15 に示すように、東日本大震災以前から、65.1%の企業がバックアップからの復旧手順を整備している。一方、「東日本大震災以降、手順を整備しはじめた」企業が 5.2%、「特に手順を整備していない」企業も 25.7%存在する。

また、手順を整備している企業において、震災時、手順やルール通りの対応ができたかどうかについては、図 2-16 に示すように、「できた」と回答した企業が 30.1%であり、「だいたいできた」とする企業が 38.7%であった。また、「できなかった」(3.4%)、「あまりできなかった」(2.1%)とする企業もあわせて 5.5%存在した。全体としては、おおむね手順どおり対応できているものの、改善の余地を残す企業も一定数存在する様子がうかがえる。これは「(1)対策実施計画」で取り上げた日経 BP 社の調査で、システム環境の災害対策において、「災害発生時のシステム復旧手順」の見直しはもっとも多くの企業が実施したい事項として挙げていることからもうかがえる点である。



○調査時期:2011 年 5 月

○調査対象(集計対象):売上高 1 億円以上の企業に勤務(もしくは経営し)、かつ社内情報システム全般について選定ないしは最終決裁を担当する 600 名、そのうち図 2-15(左図)については東日本大震災以前の基幹バックアップについて「行っていた」と回答した 501 名、図 2-16(右図)については図 2-15(左図)で「東日本大震災以前から手順を整備していた」と回答した 326 名

○調査方法:インターネット形式、いずれも単数回答

出所:株式会社矢野経済研究所『東日本大震災後の災害対策ソリューション市場』(2011 年 6 月)

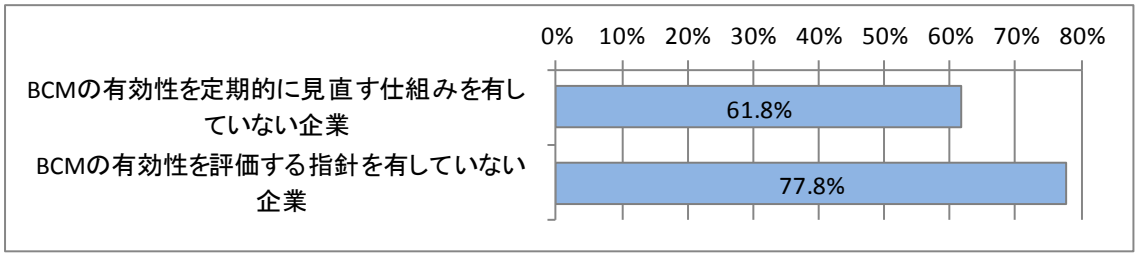
図 2-15 バックアップからの復旧手順等の整備状況　図 2-16 東日本大震災発生時の手順・ルール通りの対応

(4) 維持改善計画

「IT サービス継続ガイドライン」では、IT サービス継続の継続的な改善プロセスを明確化し、維持改善計画として定める旨を示している。これに関連して文献調査からは、IT サービス継続に関する維持改善についての調査結果は得られなかった。ここでは、文献調査で得られた IT に限定しない BCM

の維持関連に関する調査結果を示す。

インターリスク総研が実施した事業継続マネジメントに関する調査によると、図 2-17 に示すように、上場企業でも「BCM の有効性を定期的に見直す仕組みを有していない企業」は 61.8%、「BCM の有効性を評価する指針を有していない企業」は 77.8%を占めている。上場しているような大企業でも、BCM における維持改善の取り組みはあまり進んでいない様子がうかがえる。



○調査時期：2011 年 8 月～9 月　○調査対象：日本の全上場企業 3,209 社（ただし被災地に本社を置く企業は除く）

出所：インターリスク総研「第 5 回事業継続マネジメントに関する日本企業の実態調査」「東日本大震災から 1 年」（2012 年 3 月）より作成

図 2-17 BCP 策定後の取り組み

2.1.4 企業等の動向のまとめ

以上示してきた文献調査結果について、以下のようにまとめられる。

(1) IT サービス継続戦略に関する意識と変化

① 業務の IT 依存度分析

・災害対策やシステムダウンへの対応（BCP/DR）は、震災後、重要な経営課題と認識されている。
・しかし、震災を受け BCP に対する認識は高まっているものの、策定している企業は少ない（特に中小企業）。
・BCP を策定している企業が少ない実態を踏まえた上で、有効なシステム復旧対策を考える必要がある。

② IT サービス継続の要件定義

・BCP を策定している企業では、大半が重要な業務・サービスの絞りこみ、重要な業務・サービスの目標復旧時間を設定している。これらが実施されていない企業では、BCP が十分に機能していない割合が高く、これらを明確化することの重要性が示唆される。

③ リスク評価

・震災の被害の特徴として、津波により拠点施設そのものが損壊、原子力災害の発生等想定外の被害が発生した。 また、被害が長期化、広域化し、間接被害も多く発生した（電力、通信等）。

・BCP において想定するリスクとして、震災後、広域的災害、原子力災害について、多くの企業で認識されるようになった。
・IT に関しては、多くのシステムが一か所に集中していることがリスクとして認識されている。
・震災の経験を踏まえると、特定のリスクを想定して対策を実施する手法では限界があり、新たな考え方が必要になっている。

(2) IT サービス継続に向けた計画と対策の状況変化

① 対策実施計画

・システム環境の災害対策の見直しについて、災害発生時のシステム復旧手順、社内の連絡体制、ネットワーク環境の冗長性確保、別拠点への重要データバックアップ、遠隔地のバックアップサイトへのバックアップを指摘する企業が多い 。
・震災を踏まえ、クラウドについての利用を検討している企業は比較的多い。
・被災地の企業等からは、今後の IT 環境に対するニーズとして、バックアップの必要性を指摘する比率が高く、他の対策にも増してバックアップの重要性が示唆される。
・被災地に限らない企業においても震災後、基幹系システムのデータバックアップ、遠隔地バックアップとも、実施意向が強い。
・上記に示したような、企業において重要と考えている事項、懸念を踏まえ、復旧対策を考える必要がある。

② 教育訓練計画

・BCM についての教育や演習を実施している割合は大企業においても少ない。

③ 事後対応計画(緊急時対応計画)

・バックアップからの復旧手順等は半数以上で整備されている。手順どおり実施できたという企業が多いが、改善すべき点も有しているものと推察される。復旧手順の整備や確立が復旧対策のひとつのポイントになっていると考える。

④ 維持改善計画

・BCM 全般についてマネジメントシステムを構築できている企業は、大企業でも少数にとどまる。
・BCP 策定済み企業であっても、教育訓練を含め、BCM が確立できている企業が少なく、その実態を踏まえた上で、有効なシステム復旧対策を考える必要がある。

2.2 IT サービスに関連する社会インフラの被災と復旧

2.2.1 調査の概要

東日本大震災では、企業等が管理する情報システム基盤の被害とともに、IT サービス継続に深く関係する通信や電力についても大きな影響があった。ここでは通信、電力についての被災や復旧について、文献から調査を実施した。調査の概要は表 2-3 に示すとおりである。

表 2-3 文献調査(IT サービスに関連する社会インフラの被災と復旧)の概要

項目	内容
調査目的	IT サービスに関連の深い、通信、電力の東日本大震災時の被災や復旧状況について調査し、企業等が IT サービスを継続する上で留意すべき課題を探るため
調査対象	震災を受けて調査された通信、電力の被災・復旧に関する文献 ・国の報告書・白書 ・各種団体の報告書 ・インフラ事業者の公表資料 等
調査項目	・通信、電力の被災状況 ・通信、電力の復旧状況
調査時期	2012 年 3 月～4 月

2.2.2 通信の被災と復旧

(1) 被災状況

東日本大震災により、被災地である東北エリアを中心に、以下のような被害があった。

地震や津波により、通信設備について通信施設内の設備や機器の倒壊・水没・流失、ケーブルの切断や管路、電柱等の損壊、通信基地局の損壊などの大きな被害が発生した。また、停電が長期化したことにより、通信施設に備えられた非常用電源も枯渇し、通信サービスの停止が発生した。

固定通信網については、表 2-4 に示すように、NTT 東日本、KDDI、ソフトバンクテレコムの 3 社で約 190 万回線が被災した。NTT 東日本では、385 の通信ビルが機能停止している。また、携帯電話および PHS 基地局についても、表 2-5 に示すように NTT ドコモ、KDDI、ソフトバンクモバイル、イー・モバイルおよびウィルコムの 5 社合計で最大約 29,000 局が停波した。

表 2-4 固定通信の被災状況

事業者名等	被災回線数(最大) (万回線)
NTT 東日本(固定電話)	100.6
NTT 東日本(FTTH)	51.3
KDDI(固定電話)	14.1
KDDI(FTTH・ADSL)	24.9
ソフトバンクテレコム(固定電話)	3.1

出所:総務省「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」(2011 年 12 月)より作成 (掲載 URL:http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html)

表 2-5 移動通信の被災状況

事業者名等	停止基地局数(最大) (局)
NTT ドコモ	6,720
au	3,680
ソフトバンクモバイル	3,786
イー・モバイル	704
ウィルコム	13,760

出所:総務省「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」(2011 年 12 月)より作成 (掲載 URL:http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html)

今回の震災により中継網も被災した(表 2-6)。特に沿岸部の通信設備については、津波により、大きな被害が生じた。太平洋沿岸に沿って設置されている基幹回線および重要な通信施設が損傷したことにより、内陸部を含む固定通信のサービスに影響を及ぼした。移動通信も、各基地局までを結ぶ固定回線を使用しているため、固定回線の中継網の被災とともに多数の基地局で通信ができない状態となった。また、国際間の中継網についても、アジアおよびアメリカ向けの海底ケーブルが地震により切断される被害を受けた。

表 2-6 中継網のおもな被災

事業者名等	被災内容
NTT コミュニケーションズ	○中継回線断(仙台) ○アジアおよびアメリカ向け海底ケーブル断
KDDI	○東北・関東間の陸上ケーブル断 ○アジアおよびアメリカ向け等海底ケーブル複数断 ○東北以北と関東以西間の KDDI 間全通信不可

出所:総務省東北総合通信局「東北テレコムトピックス」号外 Apr.2011 より作成
(掲載 URL:http://www.soumu.go.jp/soutsu/tohoku/kohoshi/pdf/2011gogai.pdf)

(2) 通信集中による混雑

一方、震災発生時の通信集中による混雑のため、通信事業者各社は、発信規制を実施した。固定電話については、NTT 東日本、KDDI が 90%、ソフトバンクテレコムが 80%の規制を実施した。ただ

し、NTT 東日本の例では、携帯電話ほどのトラヒックの増加は発生しなかったため、通信規制は比較的早い段階で解除された。

移動通信の音声通信については、最大で NTT ドコモが 90%、KDDI が 95%、ソフトバンクが 70%の規制を実施した。他方、パケット通信については、一時、NTT ドコモのみが 30%の規制を実施したが、すぐに規制は解除された(表 2-7)。

表 2-7 通信集中による混雑

種別	事業者名等	発信規制値(最大)(%)
固定通信	NTT 東日本 ＊1	90
	KDDI	90
	ソフトバンクテレコム	80
移動通信	NTT ドコモ(音声) ＊2	90
	NTT ドコモ(パケット)	30
	au(音声)	95
	au(パケット)	0
	ソフトバンクモバイル(音声)	70
	ソフトバンクモバイル(パケット)	0
	イー・モバイル	発信規制非実施

*1 通常時の約 4～9 倍の通信量が発生。 *2 通常時の約 50～60 倍の通信量が発生。
出所:総務省「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」(2011 年 12 月)より作成 (掲載 URL:http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html)

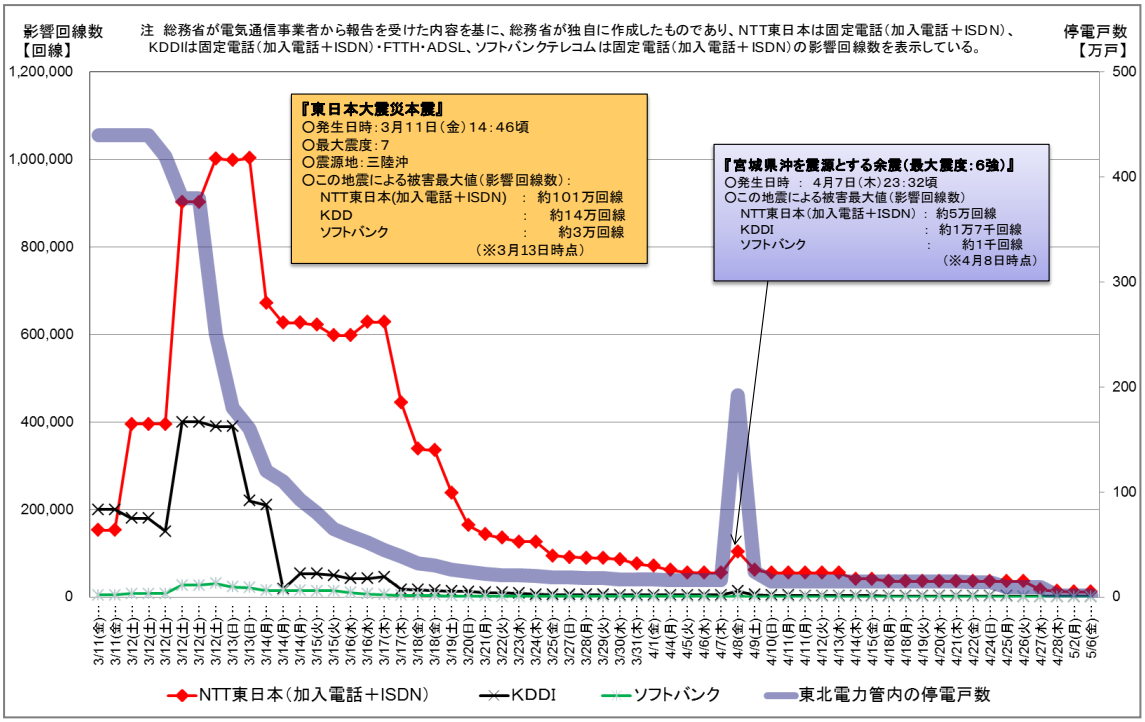
(3) 復旧状況

固定通信事業者は、屋外設置型回線収容装置の設置や、隣接ビルからの他局収容(他エリアからのケーブル敷設やネットワーク設備の張出し)等を実施した。

移動通信事業者は、基地局の被災に対して、既存基地局の大ゾーン化、移動基地局や小型基地局(フェムトセル)の設置等を実施した。

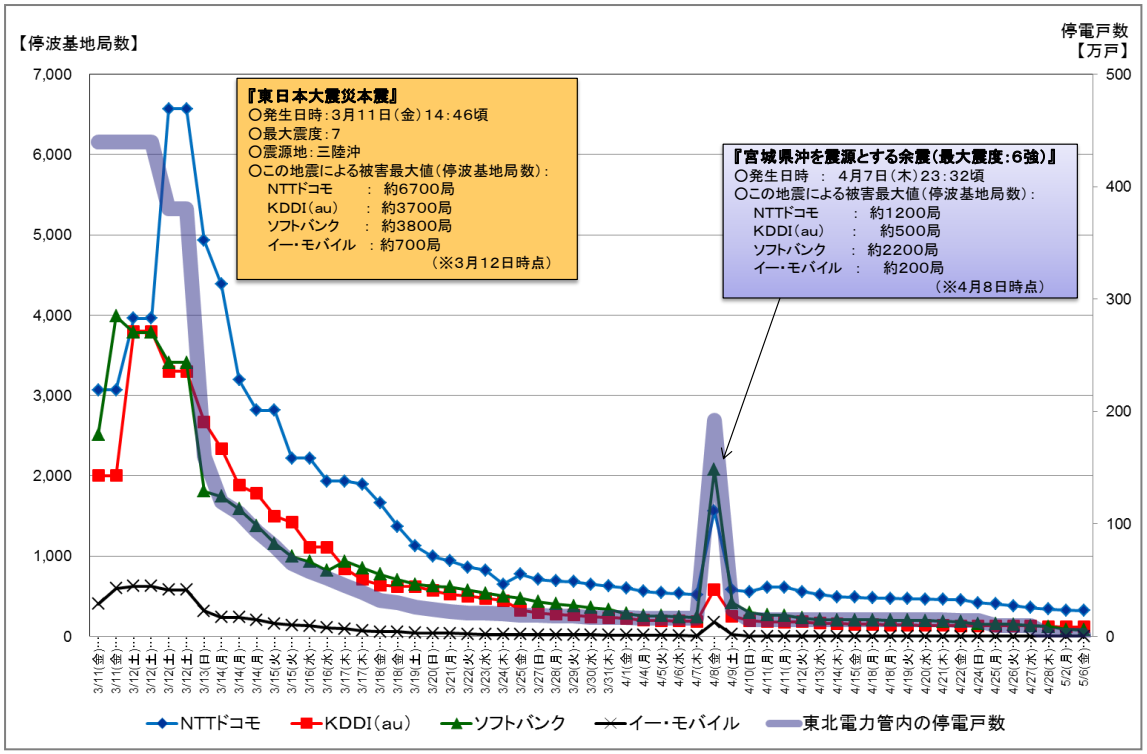
また、中継網の被災に対しては、通信事業者各社は、基幹回線の迂回措置をとるとともに、一部回線についてはマイクロ波や衛星回線を活用するなどの対策を実施した。国際間においても、海底ケーブルの被災に対して、迂回措置による応急対策が行われた。

図 2-18、図 2-19 に示すように、これらの応急・復旧対策を実施した結果、影響回線数は 2～3 日で半減した。最終的に、2011 年 4 月末までに一部地域を除き、ほぼ復旧した。



出所：総務省「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」（2011 年 12 月）
（掲載 URL：http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html）

図 2-18 固定電話の影響回線数の推移



出所：総務省「大規模災害等緊急事態における通信確保の在り方について最終とりまとめ参考資料」（2011 年 12 月）
（掲載 URL：http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000043.html）

図 2-19 携帯電話基地局の停波基地局数の推移

2.2.3 電力の被災と復旧

(1) 発電所の被害

震災の発生を受け、表 2-8 に示すような主な発電所が停止した。このため、東日本における電力の供給力が大幅に低下した。経済産業省資源エネルギー庁「平成 22 年度 エネルギーに関する年次報告」によると、東京電力の供給力は、約 2,100 万 kW が欠落(約 5,200 万 kW から約 3,100 万 kW へ約 4 割減)した。この結果、東京電力管内のこの時期のピーク時の想定需要量約 4,100 万 kW に対し、約 1,000 万 kW の大幅な供給力不足が発生した。東北電力の供給力は、約 500 万 kW が欠落(約 1,400 万 kW から約 900 万 kW へ約 3.5 割減)した。

表 2-8 停止した主な発電所

事業者	発電所
東北電力	東通・女川・仙台・新仙台・原町
東京電力	福島第一・福島第二、広野・常陸那珂
その他	日本原電東海第二、鹿島共同火力

出所:経済産業省資源エネルギー庁「平成 22 年度 エネルギーに関する年次報告」(平成 23 年 10 月)より作成
(掲載 URL:http://www.enecho.meti.go.jp/topics/hakusho/2011/index.htm)

(2) 停電の発生

震災による変電所などの流通設備への影響等により、東京電力および東北電力管内を中心に広範囲にわたり停電が発生した。東北電力管内においては約 466 万戸、東京電力管内においては約 405 万戸の停電が地震発生直後に発生した。(表 2-9)

表 2-9 停電の状況

事業者	延べ停電戸数(最大)
北海道電力	約 3 千戸
東北電力	約 466 万戸
東京電力	約 405 万戸
中部電力	約 4 百戸

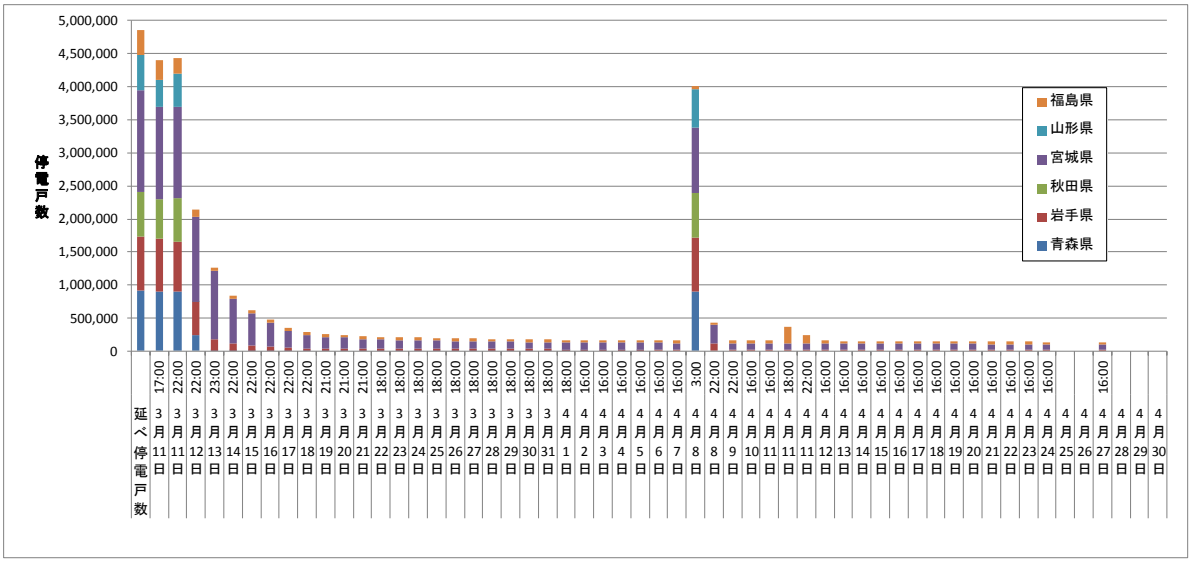
出所:経済産業省原子力安全・保安院「地震被害情報(第 64 報)」(2011 年 3 月 31 日)より作成
(掲載 URL:http://www.meti.go.jp/press/20110331001/20110331001.html)

(3) 復旧状況

東北電力と東京電力における停電の解消の推移を図 2-20、図 2-21 に示す。

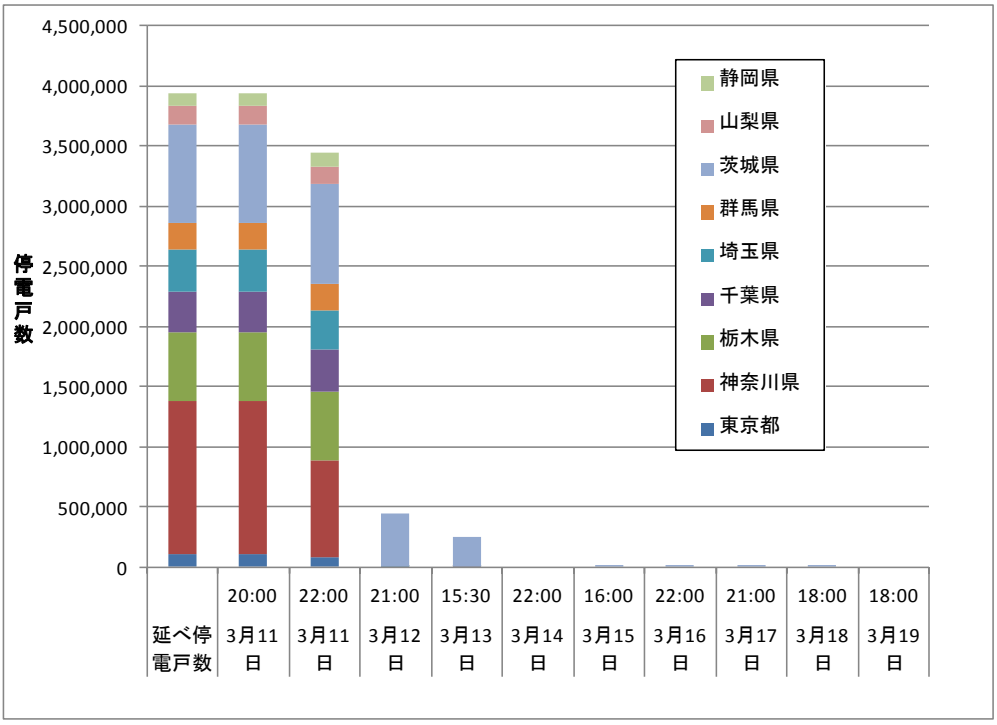
東北電力管内では、停電戸数が半減するのに 1～2 日間を要している。以降は、4 月 8 日の余震で再び停電が発生するも、震災発生 1 か月後には一部地域を除き解消している。

東京電力管内では、停電は、翌日には茨城県を除きほぼ解消し、茨城県においても 3 月 19 日には解消している。



出所：岐阜大学工学部社会基盤工学科教授能島暢呂「東日本大震災におけるライフライン復旧概況（時系列編）」（2011 年 6 月）（掲載 URL：http://committees.jsce.or.jp/2011quake/node/86）

図 2-20 停電戸数の解消過程（東北電力管内）



出所：岐阜大学工学部社会基盤工学科教授能島暢呂「東日本大震災におけるライフライン復旧概況（時系列編）」（2011 年 6 月）（掲載 URL：http://committees.jsce.or.jp/2011quake/node/86）

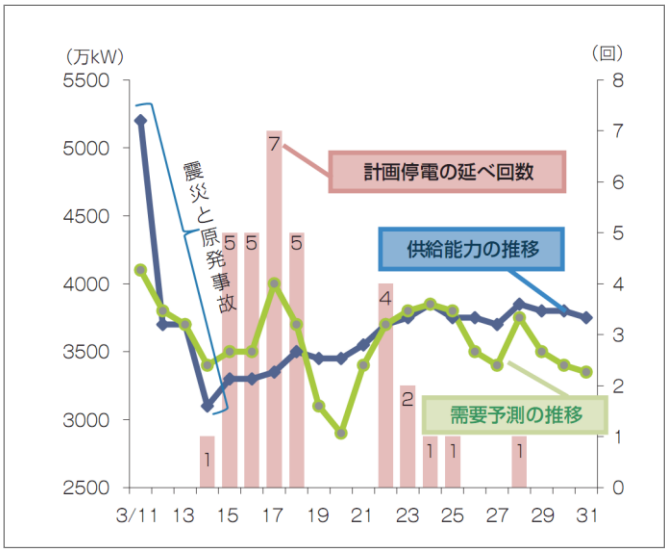
図 2-21 停電戸数の解消過程（東京電力管内）

(4) 計画停電・電力使用制限

東京電力管内における電力供給力不足に対する方策として、系統の変電所に則したエリア毎に順次停電させる計画停電による対応が行われた。

図 2-22 に示すように、2011 年 3 月 14 日から 28 日の間の計 10 日間、延べ 32 回実施された。この結果、首都圏の企業等における情報システムの運用にも非常に大きな影響を与えた。

また、電力需要が高まる夏季において、東京電力、東北電力管内で、電気事業法第 27 条に基づく電力使用制限令が発動された。これにより、7 月 1 日から 9 月 9 日（東京電力管内では当初 9 月 22 日までであったが緩和された）までの平日 9:00～22:00 の間、消費電力前年ピーク時比 15%削減が求められた。



出所：経済産業省資源エネルギー庁「平成 22 年度　エネルギーに関する年次報告」（平成 23 年 10 月）
（掲載 URL：http://www.enecho.meti.go.jp/topics/hakusho/2011/index.htm）

図 2-22　東京電力管内の計画停電の実施回数

2.2.4 通信・電力インフラの被災と復旧のまとめ

以上みてきたように、東日本大震災では、広い範囲で通信サービスや電力供給サービスが停止し、停止の状況が半減するまでに1～3日を要し、全面的に復旧するまでには1か月間程度を要している。また、原子力発電所の事故以降、電力供給には不安を残しており、今後も、電力使用制限等が実施される可能性もある。

情報システム基盤の復旧対策の向上のためには、長期的、広域的に通信サービスや電力供給サービスが停止することに備えた対策が必要である。

3　新しい技術・サービスの活用

3.1 新しい技術・サービス

3.1.1 調査の概要

東日本大震災では、被災して情報システムを利用できなくなった組織が、ベンダなどが提供するクラウドサービスなどを利用して業務を行った事例が多くみられた。また、これまで遠隔地にバックアップデータの保管を行っていなかったり、災害時の情報システムのバックアップサイトを保有していなかったりした組織が、震災をきっかけとしてクラウドサービスなどをバックアップデータの保管先やバックアップサイトなどに活用しようとする動きも出つつある。このような傾向を踏まえ、クラウドサービスとその前提技術となるサーバ仮想化技術に着目し調査を実施した。調査の概要は表 3-1 に示すとおりである。

表 3-1　文献調査（新しい技術・サービス）の概要

項目	内容
調査目的	サーバ仮想化およびクラウドサービスにおけるバックアップ、システム復旧、災害対策に関わる技術・サービスについて調査し、企業等が IT サービスを継続する上で有効な活用方法等を探るため
調査対象	IT、システムに関する文献 ・各種団体、民間企業の報告書 ・専門書籍・雑誌 ・ベンダ、サービス事業者の公表資料（Web）等
調査項目	・サーバ仮想化技術におけるバックアップ、システム復旧、災害対策技術 ・国内で利用可能なデータセンタおよびクラウドサービスにおけるバックアップ、システム復旧、災害対策サービス
調査時期	2012 年 3 月～4 月

3.1.2 新しい技術

近年はサーバ仮想化技術を導入する企業・団体が増加している。サーバ仮想化技術はクラウドサービスにおいても利用されている技術であり、クラウドサービスとの親和性も高い。現在、仮想化ハイパーバイザーのラインナップが出そろい、製品間の競争が激化するなど、仮想化技術は普及期に突入している。特に、高可用性機能および災害対策機能が充実しており、サーバ仮想化技術の活用により、従来の技術よりも効率的に高回復力システム基盤を構築できる可能性がある。本報告書では、

仮想化技術を中心に、サーバ高可用性対策およびバックアップサイト構築に役立つ技術に着目し調査を実施した。

(1) サーバ仮想化技術における IT サービス継続対策

① 高可用性機能

高可用性機能は、複数の物理サーバを用いて仮想化環境を構築しておくことにより、ハードウェア障害等発生時には、実行中の仮想サーバ(以下、「VM」とする)を別の物理サーバに切り替えることができる技術である。高可用性機能の利用にあたっては、複数物理サーバから共有可能なストレージを利用し、VM イメージをストレージに保存できるようにした上で、複数のサーバからアクセスできるようにしておくことが一般的である。この技術により、サーバ仮想化環境において、物理サーバによる二重化やクラスタリングと同等の信頼性を確保することが可能となる。高可用性機能のイメージを図 3-1 に示す。

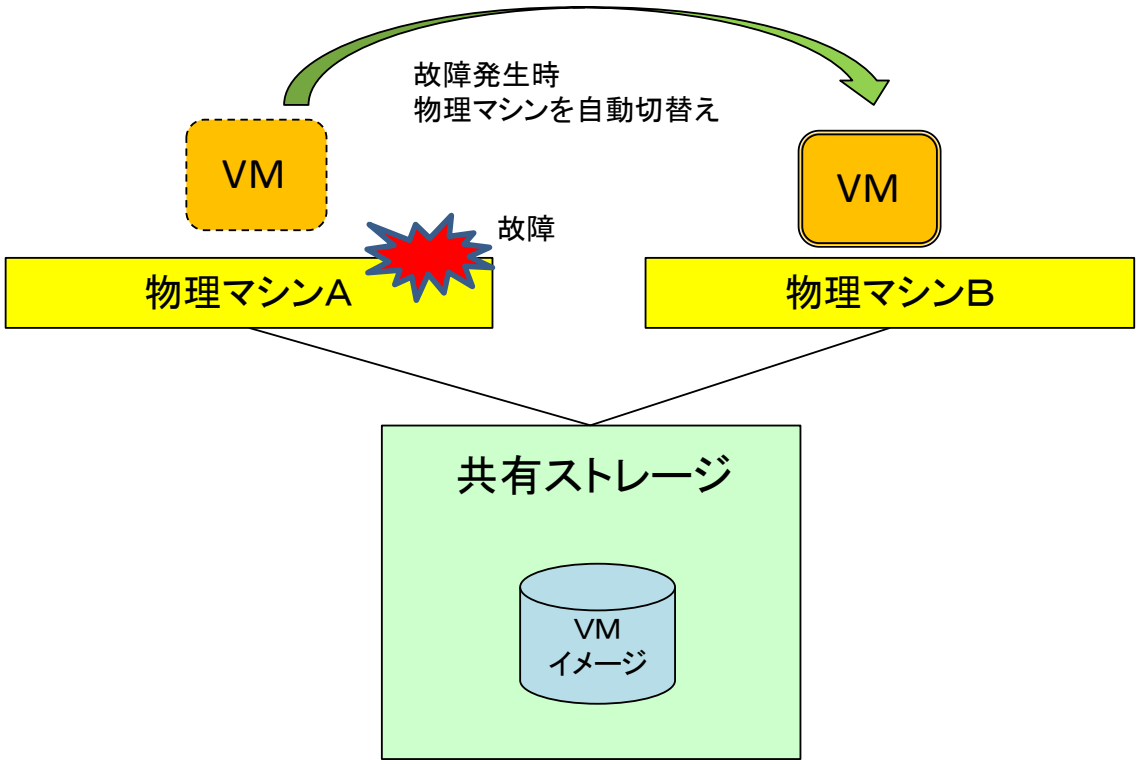


図 3-1 高可用性機能のイメージ

② 災害対策機能

高可用性機能は、共有ストレージにより VM イメージを共有する環境を前提としているため、異なる拠点にある物理サーバ間では利用できなかった。したがって、災害対策として遠隔地に待機系マシンを設置することはできなかった。近年の仮想化ソフトウェアでは、平常時から遠隔地に設置したサーバに VM のイメージコピーを実施しておき、ハードウェア故障時はこの VM イメージコピーを利用することで、停止時間を極めて短くする機能が提供されるようになってきている。これにより、仮想サーバ環境におけるバックアップサイト構築が、従来よりも容易に実現可能となってきた。災害対策機能のイメージを図 3-2 に示す。

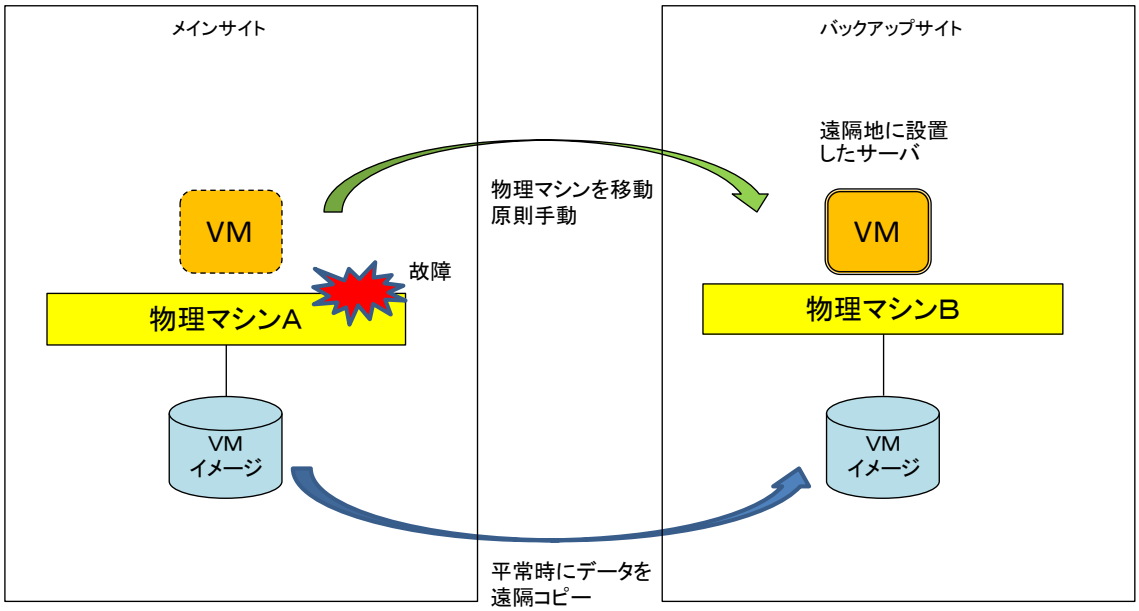


図 3-2 災害対策機能のイメージ

(2) 遠隔バックアップ高速化技術

先に紹介した災害対策機能を利用するにあたり、目標復旧時点(RPO)を高いレベルとするためには、VM イメージコピーの間隔を短縮する必要がある。企業のサーバの VM イメージはテラバイト単位になることも多く、このような大容量のデータを短時間で転送するための技術が求められる。

① 重複排除機能

重複排除機能は、バックアップ対象データから繰り返し出現するデータを一つにまとめる機能である。ハードディスクおよびストレージをバックアップの格納先とした場合は、大幅に使用量を削減することができる。また、重複排除機能を利用して遠隔バックアップを実施した場合は、WAN を経由するトラフィックが圧縮される。これにより、バックアップデータの転送時間を大幅に短縮できる。

バックアップにかかる時間が短縮されることにより、バックアップの周期を短縮することもできる。こ

れにより、障害が発生してもデータが消失するリスクは低減される。重複排除機能は、ストレージの持つバックアップ機能として提供される場合と、バックアップ専用ソフトウェアの機能として提供される場合がある。ストレージのバックアップ機能の場合、異なるストレージベンダ間では互換性が無い場合がある。重複排除機能のイメージを図 3-3 に示す。

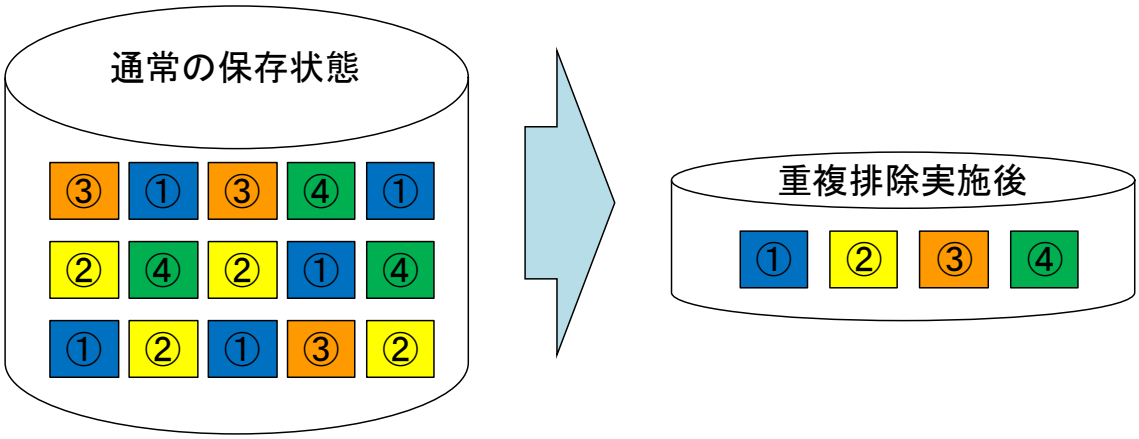


図 3-3 重複排除機能のイメージ

(3) バックアップアプライアンス

バックアップ専用のアプライアンス型製品である。製品数は少ないが、今後製品が増加してゆくことが期待される。

平常時は、ネットワーク経由でのバックアップ専用機として動作し、仮想サーバのイメージコピーおよび物理サーバのイメージコピーをネットワーク経由で取得する。バックアップはハードディスクに保存される。アプライアンスには、ハイパーバイザが搭載されており、本番機にて障害が発生した場合は、バックアップのイメージを利用して、アプライアンスが仮想サーバの動作環境となり、業務継続が可能となる。バックアップアプライアンスのイメージを図 3-4 に示す。

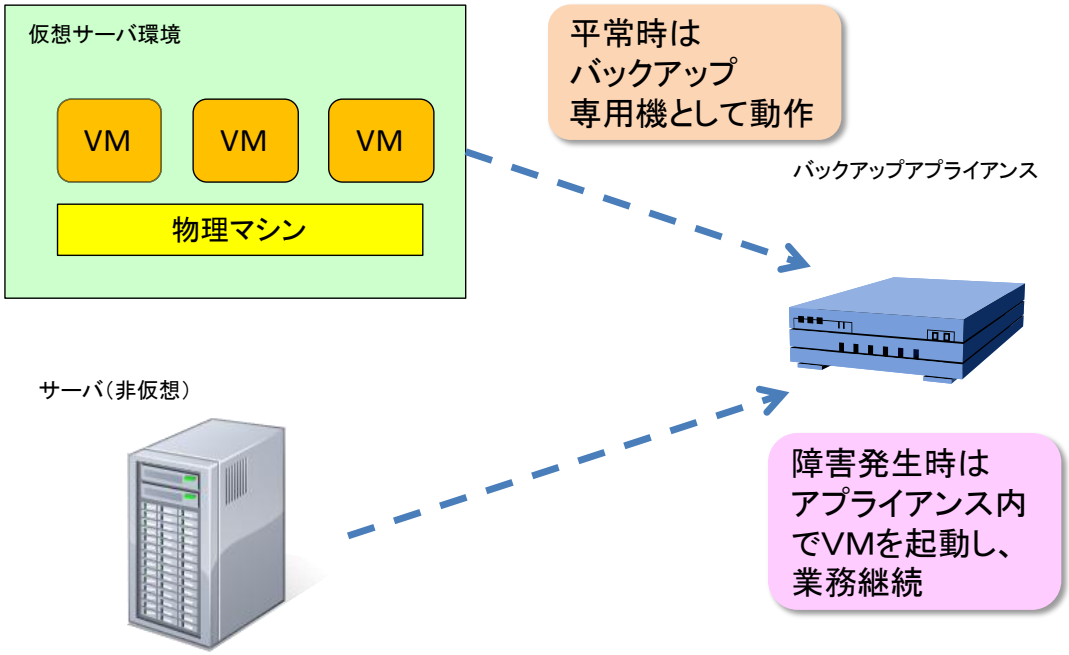


図 3-4　バックアップアプライアンスのイメージ

3.1.3 新しいサービス

自社にサーバを設置せずデータセンタにサーバを設置することおよび、クラウドサービス（IaaS/PaaS/SaaS）を利用することは、災害対策上有効である。データセンタは通常の建築物よりも堅牢であり、各種災害および停電対策等が充実している。なお、一般的なクラウドサービスについては、多くの資料書籍で紹介されているため、本報告書ではバックアップを中心としたデータセンタ／クラウドサービスについて調査を実施した。

本調査では、バックアップデータの確実な保管を実現する観点から、主にデータセンタ／クラウド側にバックアップを保存するサービスを中心に調査を実施した。

(1) 遠隔バックアップサービス

主に自社をメインサイトとする場合に、VPN や WAN 回線等を経由し、データセンタ内にバックアップデータを保管するサービスである。サービス形態としては大きく次に示す 3 パターンに分類できる。サービス条件等は、サービス事業者により異なるため、必要とされる要件を満たしているか導入する前に確認が必要となる。

① 専用型遠隔バックアップサービス

データセンタ内に設置された専用のバックアップ管理サーバを利用し、VPN や WAN 回線等経由でバックアップを行うサービスである。専用サーバであるため、バックアップ要件（バックアップ周期、バックアップ単位、バックアップ容量等）については制約が少ない場合が多い。専用型遠隔バックアップサービスのイメージを図 3-5 に示す。

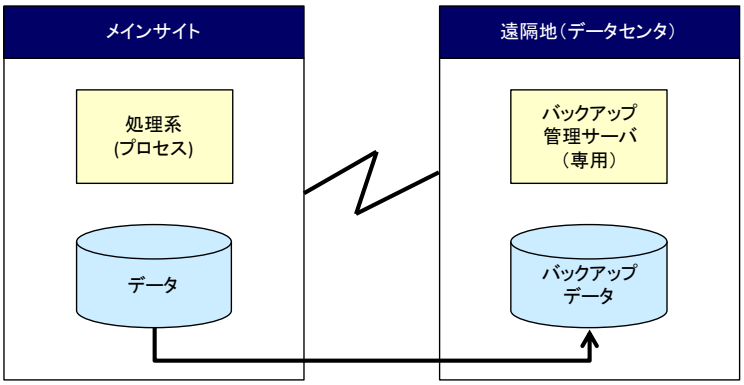


図 3-5 専用型遠隔バックアップサービスイメージ

② 共用型遠隔バックアップサービス

主に自社内にメインサーバを設置するケースにおいて、サービスプロバイダが提供する共用型バックアップ管理サーバを使用し、WAN 回線経由でバックアップを行うサービスである。専用型バックアップサービスと比較すると、導入経費は安価に抑えられることが多いものの、バックアップ要件（バックアップ周期、バックアップ単位、バックアップ容量等）については制約があることもある。共用型バックアップサービスイメージを図 3-6 に示す。

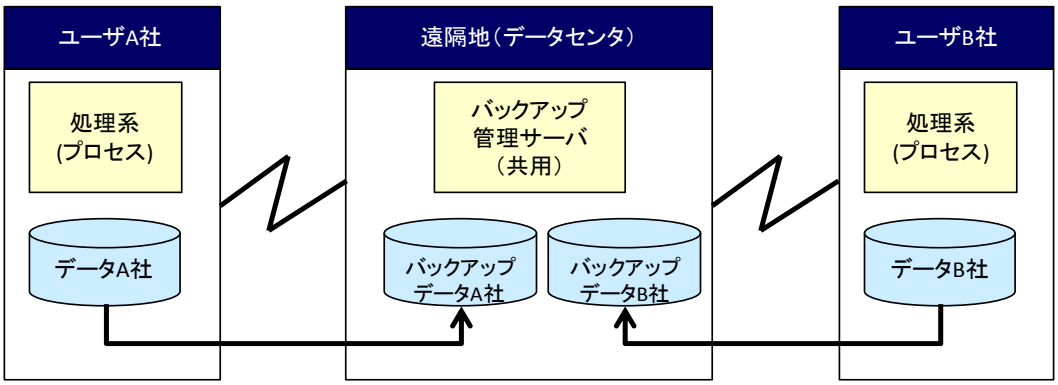


図 3-6 共用型遠隔バックアップサービスイメージ

③ ストレージベンダ限定遠隔バックアップサービス

ストレージベンダを限定した遠隔バックアップサービスである。システム形態としては共有型だが、ストレージベンダを限定しているため、先述した重複排除機能のように異なるベンダのストレージ間では利用できないストレージベンダ固有のバックアップ機能を利用できるケースもある。ストレージベンダ限定遠隔バックアップサービスのイメージを図 3-7 に示す。

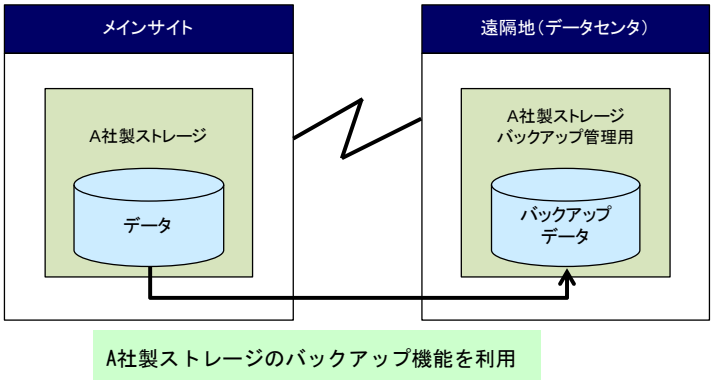


図 3-7 ストレージベンダ限定遠隔バックアップサービスイメージ

(2) データセンタ／クラウドの付加サービス

データセンタやクラウドサービスにおいては、バックアップや災害対策の付加サービスが充実しつつあり、次に示すような大きく 3 つのパターンに分類できる。利用できるサービスはサービス事業者によって異なる。

① 同一データセンタ内のバックアップサービス

データセンタやクラウドサービスに保管されたデータを、同一データセンタ内でバックアップし保管するサービスである。イメージを図 3-8 に示す。

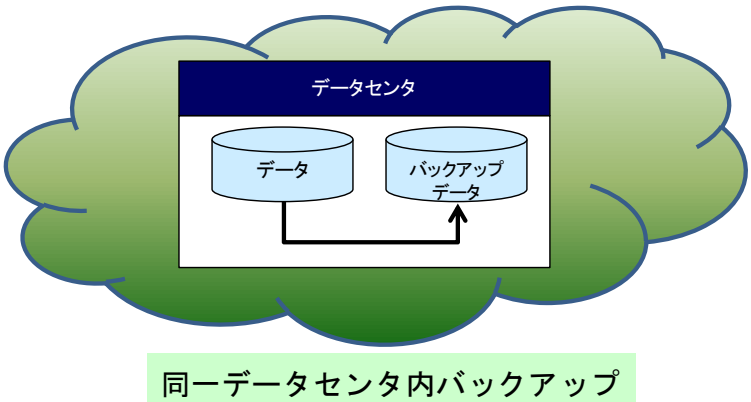


図 3-8 同一データセンタ内のバックアップサービスイメージ

② 複数データセンタ間のバックアップサービス

データセンタやクラウドサービスに保管されたデータを、異なるデータセンタに設置された別サーバにバックアップするサービスである。イメージを図 3-9 に示す。

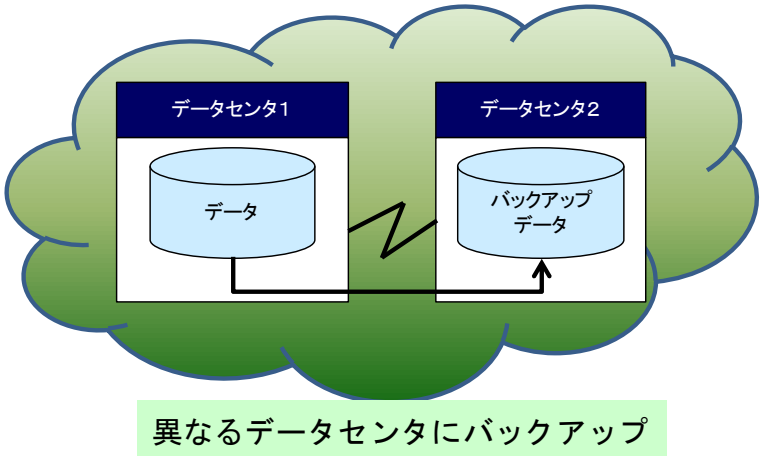


図 3-9 複数データセンタ間のバックアップサービスイメージ

③ バックアップサイトサービス

複数データセンタにサーバを設置し、片方をバックアップサイトとして運用できるサービスである。イメージを図 3-10 に示す。

さらに、以下のような機能を利用できるサービスもある。

・ハードウェア故障時は、自動的にサーバの切り替えが行われる。

・サーバ切り替え後もサーバの IP アドレスが変更されず、ユーザはサーバ切り替えが発生したことを意識せず継続利用が可能である。

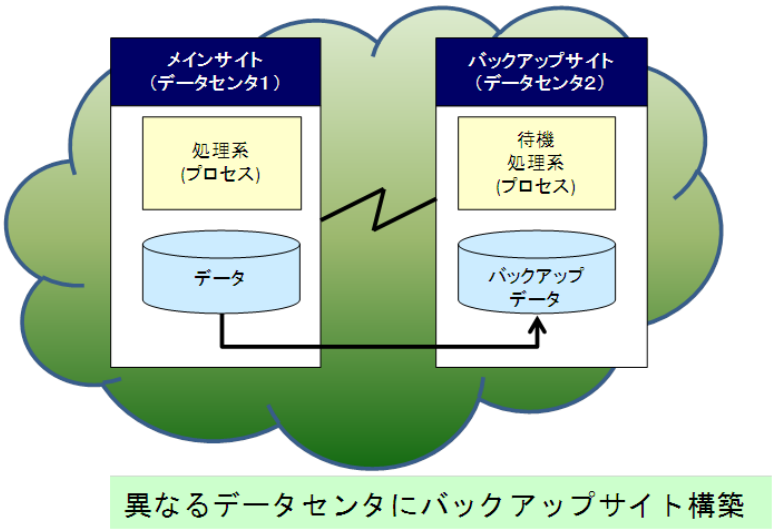


図 3-10 バックアップサイトサービスイメージ

(3) クラウドを利用したバックアップサイト構築

データセンタのサーバホスティングや IaaS 等のクラウドサービスを利用する場合、自由にソフトウェアをインストールすることができるので、これを利用してバックアップサイトを構築することもできる。イメージを図 3-11 に示す。

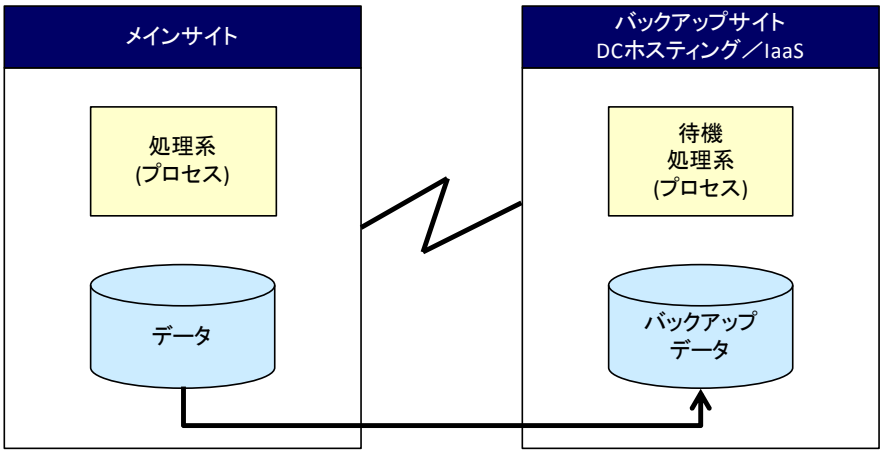


図 3-11 クラウドを利用したバックアップサイト構築イメージ

3.2 新しい技術・サービスの有効性

3.2.1 新しい技術・サービスの活用方法

(1) 同一サイト内の信頼性向上に有効な技術・サービス

同一サイト内でサーバ仮想化環境を構築し先に説明した高可用性機能を活用することで、従来から存在する技術と同等の信頼性を実現することができる。従来からある二重化やクラスタリングでは、アプリケーション単位で切り替えを行うため、設計・検証等の動作環境を整備するための作業量が膨大であったが、サーバ仮想化環境では VM 単位で切り替えが行われ、制御はハイパーバイザが行うため比較的容易に動作環境を整備することができる。イメージを図 3-12 に示す。

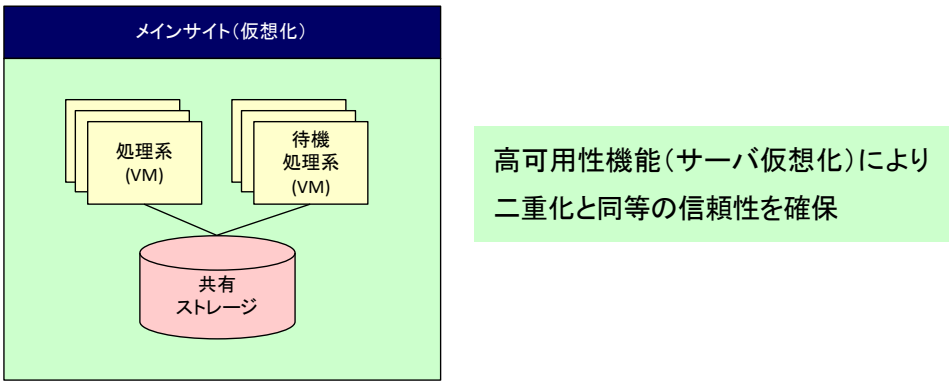


図 3-12 同一サイト内の信頼性向上に有効な技術サービスイメージ

(2) 遠隔地へのバックアップに有効な技術・サービス

遠隔バックアップサービスを利用することで、複数拠点を持たない企業や堅牢なビルやサーバルームが不足している企業であっても、遠隔地の堅牢なビルにバックアップを保存することができる。これにより、サーバを設置した建物が火災や浸水等による被害を受けても、バックアップデータが消失することを防止できる。また、バックアップの正常終了確認や媒体交換および管理が軽減される効果もある。

遠隔地へのバックアップを実施するにあたり、重複排除機能が利用できる環境であれば、WANトラフィックを軽減することができる。これにより、以下のような効果が期待できる。

・WAN 回線の条件が変わらなければ、バックアップに要する時間が短縮されることで、より大量データを扱うことが可能となる。

・データ量が変わらなければ、より低帯域で安価な WAN 回線による遠隔バックアップの実現が可能となる。

データセンタ／クラウドサービスを利用している場合に、同じデータを異なるデータセンタに設置された複数のサーバに保管するサービスを利用していれば、遠隔地へのバックアップをしている場合と、同等の効果がある。イメージを図 3-13 に示す。

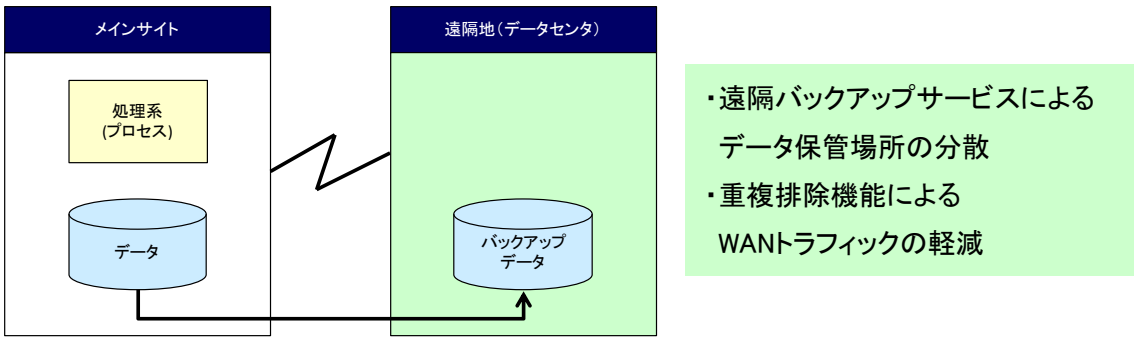


図 3-13 遠隔地へのバックアップに有効な技術・サービスのイメージ

(3) バックアップサイトの構築に有効な技術・サービス

仮想環境を利用しない場合、バックアップサイトを構築する際に、ハードウェア・ソフトウェアともにメインサイトとほぼ同等のシステムを導入し、メインサイトからのデータバックアップを行う環境を構築する必要がある。一方で、仮想化環境における災害対策機能を利用した場合、VM 単位(OS・アプリケーション・データをひとまとめ)でイメージコピーを行うため、従来技術と比較し容易にバックアップサイトを構築できる。

遠隔地にバックアップサイトを構築するにあたっては、新たなサーバを導入し設計構築を実施する等、費用が高額となることもある。しかし、比較的小規模なバックアップサイトであれば、バックアップアプライアンス製品を利用することで、比較的容易かつ安価(ハードウェアを含めて数百万円～1 千万円前後)に構築が可能である。また、メインサイトがサーバ仮想化環境でなくとも導入できる。

オフィスビルの災害対策に不安がある場合は、バックアップサイトとしてデータセンタを利用することに加え、メインサイトにおいてもデータセンタを利用ことすることもデータを確実に保管する観点から有効である。

なお、IaaS 等のサービスを利用してバックアップサイトを構築することも想定される。クラウドサービスの中には、従量課金制のサービスもあり、利用時間やデータ転送量で課金されるサービスもある。これを利用した場合、平常時はバックアップ用途でしか利用されないため、利用時間は非常に短いものとなる。データ量によっては、遠隔バックアップの専用サービスを利用するよりも、安価に利用できる場合もある。イメージを図 3-14 に示す。

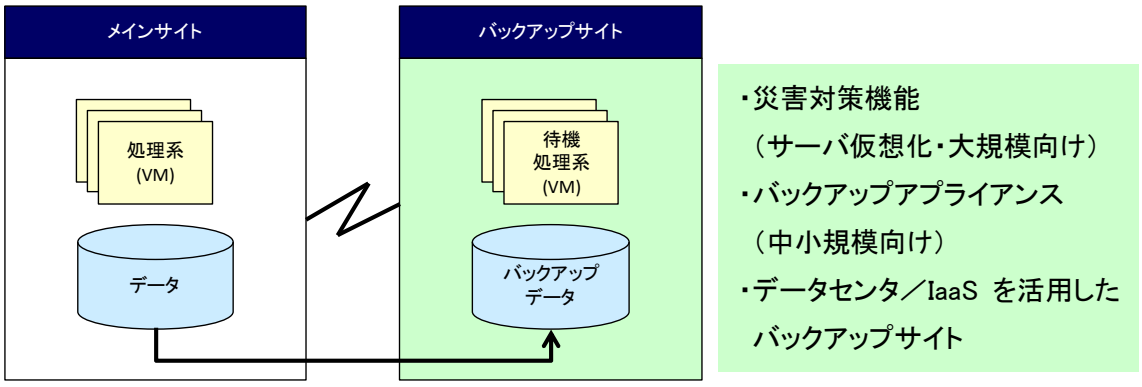


図 3-14 バックアップサイトの構築に有効な技術・サービスのイメージ

(4) 技術の組み合せによる高信頼性環境の構築

サーバ仮想化環境を導入し、以下の技術を組み合わせて使用することにより非常に信頼性および災害耐性の高いシステム環境を構築可能となるので、例として記載する。

・メインサイトにおいて高可用性機能（仮想化）を適用し、ハードウェア故障時は自動的に切り替え
・災害対策機能（仮想化）を利用したバックアップサイトにより、災害時も短時間で切り替え
・遠隔バックアップには重複排除機能を適用し、例えば 1 時間周期のバックアップを実施

イメージを図 3-15 に示す。

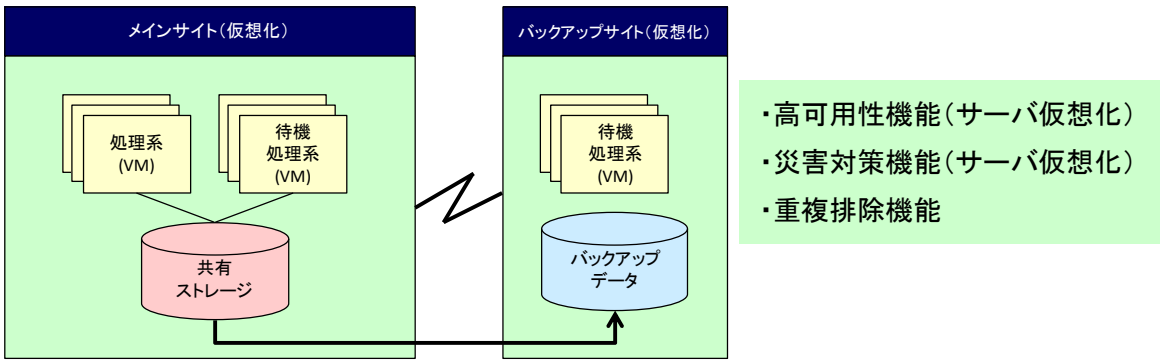


図 3-15 高信頼性環境のイメージ

3.2.2 新しい技術・サービスに関する留意点

(1) サーバ仮想化に関する留意点

① ソフトウェアの動作保障等

サーバ仮想化環境を導入するにあたり、市販ソフトウェアであっても仮想化環境において動作が保証されないケースや、動作環境として OS やミドルウェアのバージョン等が制限されるケースがある。利用するソフトウェアが予定している環境で動作するか、ソフトウェアの販売元等に確認する必要がある。また、ソフトウェアを独自開発している場合やパッケージをカスタマイズしている場合は、仮想化環境へ移行する際に事前検証を実施することが望ましい。事前検証の際に不具合が発見されることにより、ソフトウェア修正が発生するリスクがある。

② 市販ソフトウェアのライセンス体系

市販ソフトウェアの中には、稼働するサーバの CPU 個数分ライセンス購入を必要とするものがある。これらのソフトウェアを仮想化環境に導入する場合、稼働する物理サーバの全プロセッサがライセンスカウントの対象となることがある。ライセンスカウントの対象となる場合には、CPU ソケット単位で課金するものと CPU コア単位で課金するものがある。サーバ仮想化環境ではマルチソケット・マルチコア CPU を搭載した物理サーバを使用するケースが多く、ソフトウェアライセンス費用が高額になってしまう場合もあり、事前にソフトウェアの価格体系を確認する必要がある。

③ ハードウェアの制約

仮想化環境を構築するための物理サーバに、仮想化支援機能が実装された CPU が必要となることがある。この他にも、利用する製品または機能によってはハードウェア的な制約が生じることがあるため、注意が必要である。

④ レスポンスへの影響

仮想化技術はハードウェア資源を有効に活用するしくみであるが、仮想化によるオーバーヘッド処理がレスポンスに影響を与えることもあるため、ミリ秒単位の極めてシビアなレスポンスが要求されるようなシステムには適していない。また、リソース占有率の高い複数のサーバを一つの仮想化環境に統合すると、レスポンスに影響を与えることもある。このように、すべてのシステムが仮想化よる効果を得られるわけではないため、導入前の事前検討が必要である。

⑤ 運用環境の変化

仮想化を導入していない環境と仮想化環境とでは、システムの運用管理の方法が大きく異なる可能性がある。例えば、VM 単位のリソース利用状況を把握したい場合、ゲスト OS にログインしてコマン

ドを投入しても、正確な値を参照することができず、ハイパーバイザの機能を利用しなければ参照できない。一方で、アプリケーション毎のリソース利用状況を把握したい場合は、ハイパーバイザからは参照できず、ゲストOSにログインしてコマンドを投入することにより参照することができる。監視が必要なVMやアプリケーションが多い場合は、監視システムを導入して管理することも検討が必要である。この場合、監視システムは仮想化環境に対応した製品を導入しなければならない。ここで示した例のように、運用環境が大きく変わることによるシステム運用管理に関わる追加投資や人件費の増加が生じるリスクもある。

(2) 遠隔バックアップサービスに関する留意点

遠隔バックアップサービスはネットワークを経由するため、データ量によってはネットワークがボトルネックとなり、業務開始時間までにバックアップ処理が完了しない等の事態が発生することがある。したがって、バックアップのために十分なネットワーク帯域を確保する必要がある。

サービス利用するにあたり、サービス利用料だけでなくネットワーク利用料も含めて導入検討する必要がある。

なお、将来におけるバックアップデータ量の予測が困難な場合は、ネットワークがボトルネックとなり、バックアップ時間が増加し業務に影響を与えるリスク、あるいは高速なWAN回線を必要とすることによるネットワーク利用料が増加するリスクがある。

(3) クラウド利用に関する留意点

① クラウド全般における留意点

本報告書に記載したサービスはすべての事業者が提供しているものではないので、機能の有無（例えば、サーバを設置したデータセンタとは別なデータセンタにバックアップが保管されるか。）及び費用について導入前に確認する必要がある。

また、クラウドサービスの課金体系として、サーバやストレージのリソース使用料だけでなく、データ通信量にも課金するサービスがある。導入前に、十分なシミュレーションを実施しないと、想定したコストを上回るリスクがある。

クラウドサービス内における信頼性対策は、利用を開始してから改善することができない。したがって、利用を開始する前にサーバ冗長化やバックアップサイト等の信頼性対策を確認することが望ましい。なお、システム構成に関する情報が公開されない場合においては、SLA による可用性保証値を確認することが望ましい。また、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ため、停止した場合の代替手段（手作業による対応、他サービスへの切替え、同じ業者の提供する代替サービス等）も検討しておくことが望ましい。

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・セキュリティ等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等については、以下のような資料が参考になる。

・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)
・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)
・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_ver1.0.pdf)

② クラウドを利用したバックアップサイト構築に関する留意点

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サービス上で動作しなければならない。したがって、以下のような点に留意する必要があり、ここでも、事前検証の際に不具合が発見されることによる、ソフトウェア修正のリスクがある。

・クラウドサービスには、プライベートアドレスが利用できるものもあるので、メインサイトにおいてプライベートアドレスを利用している場合は、このサービスを利用しバックアップサイトにプライベートアドレスを付与することができる。
・メインサイトのサーバとクラウドサービスが提供する OS がバージョンまで含めて同じであることが望ましい。
・メインサイトで使用している DBMS 等のミドルウェアおよびパケージソフトウェアが、クラウドサービスの提供する環境で動作保障されていることを確認する必要がある。(OS の種類やバージョンに加え、クラウドサービスが使用しているハイパーバイザとバージョン等も含めて確認することが望ましい。)
・メインサイトとクラウドサービス間の遠隔バックアップ環境を構築するにあたり、動作確認を行うことが望ましい。
・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および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無い場合、クラウドサービス上での動作確認試験を実施することが望ましい。
・障害発生時の切り替え手順や通常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。特に、メインサーバとバックアップサーバ両方をオンプレミス型で構築した場合に比べ、利用できるソフトウェアが制限されることもあり、異なる手順を検討しなければならないこともある。

3.2.3 新しい技術・サービスのまとめ

サーバ仮想化技術においては、メインサイト内の信頼性向上、バックアップサイト構築に活用できる技術が充実している。従来型の技術と同等の信頼性を確保することが可能であり、しかも従来型の

技術より容易に環境を構築できる。

データセンタサービスを含むクラウドサービスについても、遠隔バックアップサービス、データセンタ内バックアップサービス等が充実している。また、複数データセンタにまたがるバックアップサービスのような災害対策も充実している。さらに、複数データセンタを利用しメインサイトとバックアップサイトを構築するといった高度な利用方法も実現可能な環境が整いつつある。

一方、サーバ仮想化技術やクラウドサービスを利用するにあたっては留意事項で触れたようなリスクも存在し、導入後に期待した効果が得られないことや、想定外の問題が発生することもある。導入にあたっては、事前に有効性評価に加え、リスク評価を実施することが重要である。

4　企業等における実態

4.1 データ保管等に関わる取り組みの実態

4.1.1 アンケート調査の概要

本アンケート調査は、上場企業および非上場の資本金 1 億円以上の企業のうち、信用調査会社が保有するデータベースの中から任意に抽出した 3,000 社を対象として行った。アンケートの依頼は、IT サービス継続や情報システム基盤の復旧対策（データのバックアップ等）に関わると思われる情報システム部門の責任者に対して行った。調査票は、郵送またはオンラインにより回収し、357 社からの回答を収集した。アンケート調査の概要は表 4-1 に示すとおりである。

表 4-1　アンケート調査の概要

項目	概要
調査目的	企業のデータ保管に関する実態を把握し、情報システム基盤の復旧対策を行う上での課題を探るため
対象企業	上場企業および非上場の資本金 1 億円以上の企業のうち、信用調査会社が保有するデータベースの中から任意に抽出した 3,000 社
調査依頼先	IT サービス継続や情報システム基盤の復旧対策（データのバックアップ等）に関わると思われる情報システム部門の責任者
調査方法	郵送による調査票の回収 およびオンラインによる Web アンケートシステムでの回答
質問数	48 問
実施期間	2012 年 4 月 1 日（日）～2012 年 4 月 18 日（水）
回答件数	357 件（回収率 11.9%）

(1) 調査対象企業選定の考え方

本調査の有用性を確保するため、情報システム基盤を構築・運用する必要性が高い企業を調査対象に選定した。具体的には、上場企業および非上場の資本金 1 億円以上の企業を調査対象企業の母集団としている。上場企業は株式市場への上場要件として事業規模が規定されていることや厳格な内部統制が求められている。そのため、事業運営を効率化するために一定以上の IT 投資がなされていることが予想され、情報システム基盤が構築されていることが期待される。また、非上場企業は一定規模以上の企業であれば相当程度の IT 投資を行っていることが考えられることから、資本金 1 億円以上の企業を母集団の対象とした。

目標回収件数を 200 件とし、期待回収率を同様調査の実績から 6.7%と設定したことから、調査対象企業を 3,000 社とした（図 4-1）。

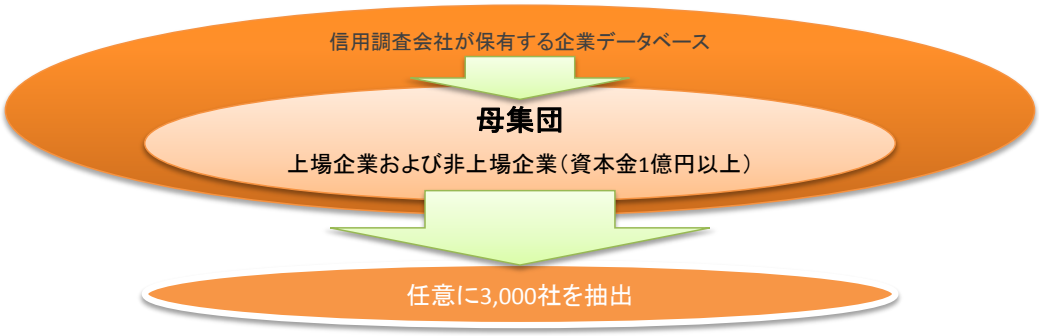


図 4-1　調査対象企業選定の考え方

(2) 調査対象企業の抽出

調査対象企業は、前述の調査対象企業選定の考え方に基づき、信用調査会社が保有する企業データベースの中から、任意の 3,000 社を抽出した。抽出に当たっては、調査対象とする企業群（上場企業および非上場企業（資本金 1 億円以上））と同様な業種構成比とした。調査対象企業と回答企業の構成業種は、図 4-2 のとおりである。

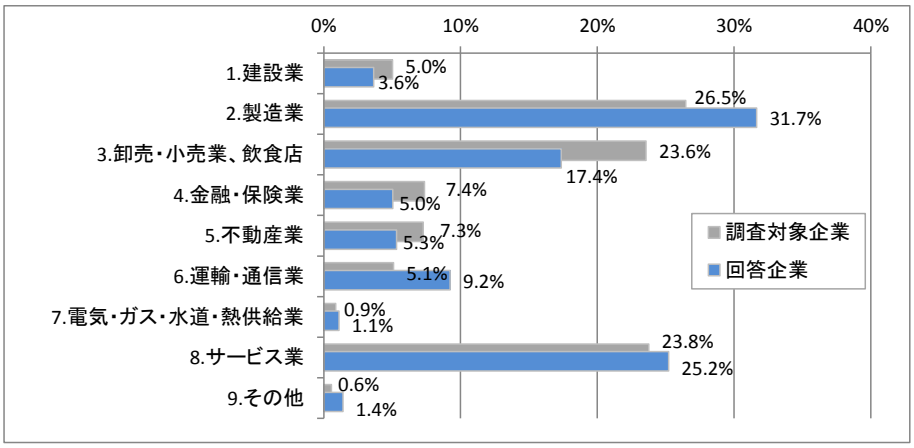


図 4-2　調査対象企業群と回答企業の構成業種

(3) アンケート調査依頼先の考え方

本調査は、情報システム部門の責任者に対して回答を依頼した。本調査は、IT サービス継続への取り組み状況や情報システム基盤の復旧対策（データのバックアップ等）についてたずねており、経営に直結する内容からIT に関する具体的な対策内容まで多岐に渡っている。一般的に、情報システム部門の責任者は、経営における IT の位置づけの検討や、情報システムにおける具体的な対策の検討を担当していることから、今回の調査の依頼先とした。

(4) 調査方法

本調査は、各企業の本社所在地宛てに調査依頼文書を郵送した。回答者の利便性に配慮して 2 種類の回答方法を用意した。1 つは、調査依頼文書に同封した調査票に回答を記載し、郵送で返送する方法である。もう1つは、Web アンケートシステムへの入力により、オンラインで回答する方法である。回答者はどちらかの方法を選択し、回答している。

(5) 調査項目

本調査は、全 48 問の質問項目で構成している。

質問内容は、データの保管(バックアップ)状況に加え、関連する事項として、IT サービス継続に関する取り組み状況やリカバリ要件定義の有無、システム構成、新しい技術やサービスの採用状況と震災被害等をたずねている(調査票は付録①を参照)。質問項目における調査対象システムは、本調査の目的に鑑み、事業継続において最も影響の大きい情報システムとした。調査項目は表 4-2 のとおりである。

なお、本調査は、調査範囲がデータの保管だけでなく、周辺の事項を広く調査対象としていることから、「IT サービス継続・情報システム基盤の復旧対策に関するアンケート調査」という名称で実施した。

表 4-2 調査項目

分類	概要	項目
①IT サービス継続に関する取り組み状況	IT サービス継続に対する意識や平常時にどのような準備や活動を実施しているか確認する	・BCP や情報システム部門における事業継続計画(以下「IT-BCP」とする。)の策定状況 ・IT サービス継続に関する活動の状況 ・想定したリスクや重点的に取り組んでいる領域
②コンピュータシステムと新しい技術の採用状況	重要な情報システムを特定し、新しい技術の採用状況を確認する	・利用しているシステムとバックアップ対象の確認 ・仮想化やクラウドの利用状況
③システム構成の冗長化	システム構成や冗長化の状況を確認する	・システムの冗長化の確認
④リカバリ要件定義の有無	サービス継続の復旧目標の設定状況を確認する	・目標復旧時間(RTO)の設定 ・目標復旧レベル(RLO)の設定 ・目標復旧時点(RPO)の設定
⑤データの保管(バックアップ)の状況	バックアップの実施状況を確認する	・バックアップポリシーの整備状況 ・バックアップの実施状況
⑥震災被害やその他の障害の経験とその後の対応	復旧対策の有効性を確認する	・被災後に不十分だと感じた対策 ・過去に復旧に失敗した事例

4.1.2 アンケート調査の結果

(1) 調査結果のポイント

① IT サービス継続に対する意識や平常時の準備や活動

IT サービス継続に対する意識や平常時の準備や活動について、事業継続計画(BCP)・情報システム部門における事業継続計画(IT サービス継続計画、IT-BCP)の策定状況や想定するリスク、情報システム基盤の復旧において重点的に取り組んでいる領域等に関する調査を行った。

a. BCP と IT-BCP の策定状況

BCP を「策定済み」としている企業は 40.1%、「未策定(検討中)」としている企業は 33.1%、「未策定(予定なし)」としている企業は 18.6%となっている。また、IT-BCP を「策定済み」としている企業は 24.8%にとどまっており、「未策定(検討中)」としている企業は 40.9%、「未策定(予定なし)」としている企業は 27.4%となっている。両者とも「策定済み」と「未策定(検討中)」を合わせて 2/3 を超えており、事業継続や IT サービス継続に対する機運が高まっているものの、両者を策定している企業は少ない。また、文献調査の結果(図 2-4)で示した企業の BCP 策定状況の傾向と一致しており、改めて事業継続への取り組みの傾向を確認することができた。

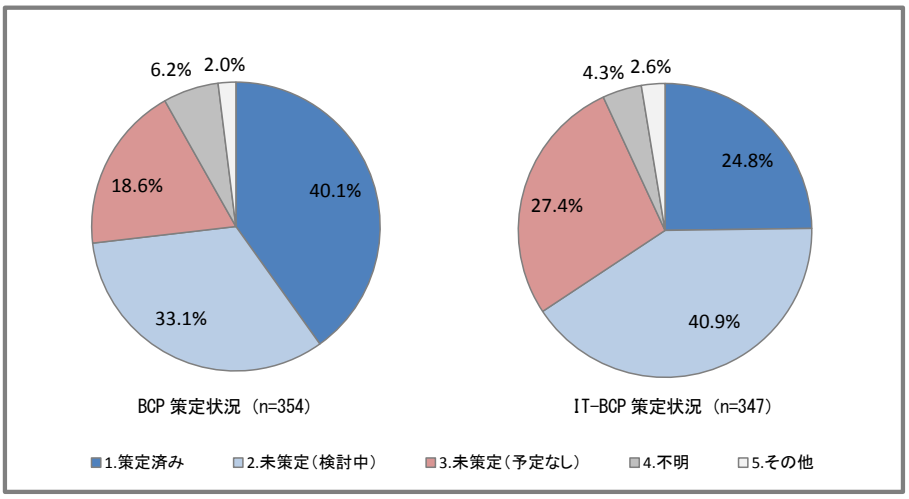


図 4-3 BCP(左)と IT-BCP(右)の策定状況

図 4-4 のとおり、BCP と IT-BCP の策定状況を比較すると、BCP の方が普及している。これは、IT-BCP に関する取り組み自体が、事業継続を支援するための取り組みと考えられていることが要因である。実際、IT-BCP 策定済みの企業では、92.9%が BCP を策定済みとなっており、IT-BCP のみ策定している企業は極めて少数派となっている(図 4-4 右)。また、BCP 策定済みの企業では IT-BCP 策定済みが 60.8%に留まっており(図 4-4 左)、事業の IT 依存度等に応じて対策を実施している実態を反映しているものと考えられる(図 4-6 右)。

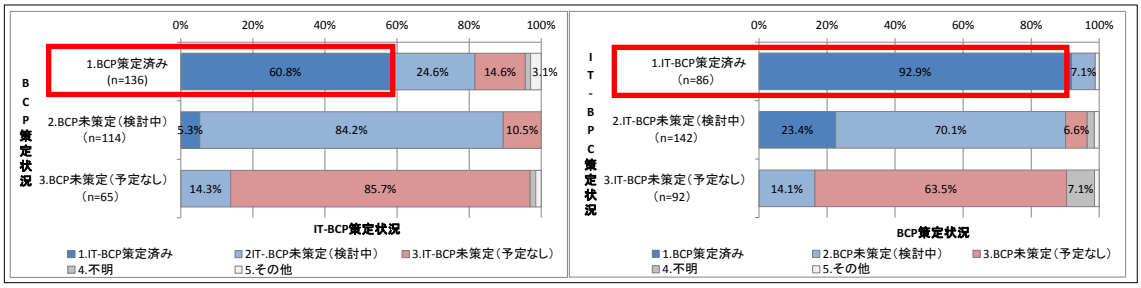


図 4-4 左:[BCP 策定状況別] IT-BCP 策定状況／右:[IT-BCP 策定状況別] BCP 策定状況

次に、事業規模別に策定状況を比較すると、資本金規模が大きいほど、BCP や IT-BCP を策定している傾向が強い(図 4-5)。これは従業員規模別にみても同様の傾向がみられた。また、IT 依存度の高さ別に比較すると、IT 依存度が高いほど策定が進んでいる様子がうかがえる(図 4-6)。事業規模が大きくなれば IT への依存度が高くなり、結果的に BCP や IT-BCP の必要性が増してくるため、両計画を策定する企業の割合が増えると考えられる。

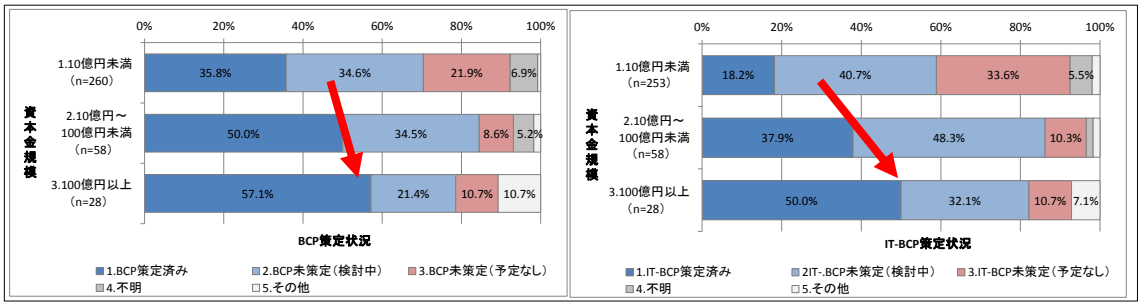


図 4-5 [資本金規模別] 左:BCP 策定状況／右:IT-BCP 策定状況

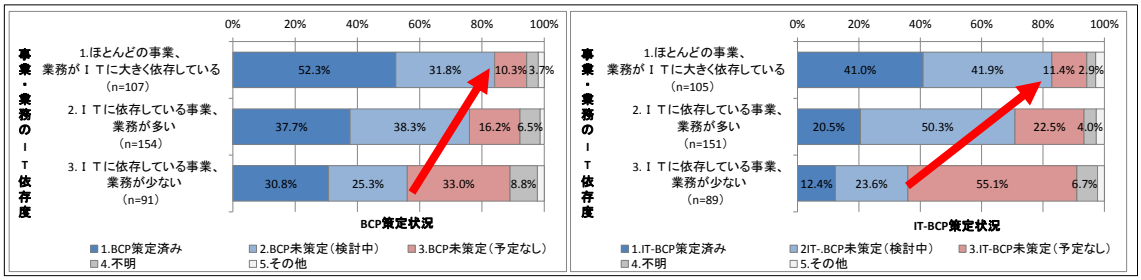


図 4-6 [事業の IT 依存度別] 左:BCP 策定状況／右:IT-BCP 策定状況

b. IT サービス継続に関する活動の状況

IT-BCP を「策定済み」または「未策定（検討中）」と回答した企業に、IT サービス継続に関する取り組み状況をたずねた。具体的には、「IT サービス継続ガイドライン（経産省）」に記載された 7 つのプロセスに沿って、その実施状況を確認した。

事業継続のために必要な IT サービスを特定している企業は 52.2%となった。その他のプロセスは、それよりも低調となっている（図 4-7）。

事業継続マネジメントにおける認証規格である BS25999-2 や ISO22301 では、ビジネスインパクト分析（BIA）の実施が要求事項となっている。ビジネスインパクト分析（BIA）は、企業活動が中断等した際の影響度を把握し、有効な計画や対策を検討するための情報を整理する、重要なプロセスである。しかし、実際にビジネスインパクト分析（BIA）を実施している企業は多くないことが分かった。本調査では、IT-BCP 策定済み企業のうち 92.9%は BCP 策定済みである（図 4-4 右）。事業継続マネジメントの考え方に則れば、大半の企業がビジネスインパクト分析（BIA）を「実施済み」となっていて然るべきであるが、25.0%の企業しかビジネスインパクト分析（BIA）を実施していない。加えて、40.4%は実施の検討も行っていない（図 4-7）。ヒアリング調査では、ビジネスインパクト分析（BIA）の実施には膨大な稼働を要するとの意見もあったことから、ビジネスインパクト分析（BIA）の普及は今後の課題だと考えられる。また、「教育訓練計画を策定」や「維持改善計画を策定」は、ビジネスインパクト分析（BIA）よりも実施率が低くなっている。これらは計画発動時の有効性を確保するために非常に重要な取り組みであり、本調査のヒアリング企業もその効果を強調している。IT-BCP の有効性を確保するためには、計画文書を準備するだけでなく、その前提となる業務の分析や要員の教育訓練、計画の継続的な見直しを行うことが重要である。

なお、IT-BCP を策定済みとしていると回答した企業にたずねているものの、いずれの取り組みも「未実施」または「不明」としている企業が散見されることから、回答者に対する IT サービス継続についての説明が充分でなかった可能性も考えられる。

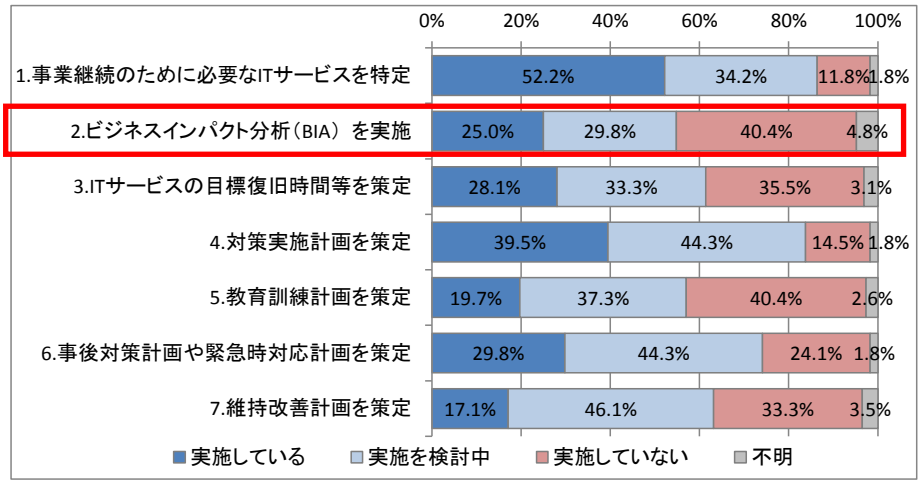


図 4-7 IT サービス継続への取り組み状況（n=228）

c. 想定したリスクや重点的に取り組んでいる領域

IT サービス継続策定時に想定するリスクは、上位から「自然災害（直下型地震による局所被害）」、「自然災害（大規模地震による広域災害）」、「停電」、「ハードウェアの故障」、「通信回線関連の故障」、「建物や施設の破壊・損失」の順となっている（図 4-8）。

業種別の想定リスクを比較したところ、全体の状況と似通った傾向はあるものの、業種によって若干の傾向の違いが見られた（表 4-3）。たとえば、建設業では「ソフトウェアの不具合」、製造業と卸売・小売業、飲食店では「停電」、金融・保険業では「ハードウェアの故障」、運輸・通信業では「建物や施設の破壊や損失」、サービス業では「通信回線の故障」がより高い比率で挙げられている。

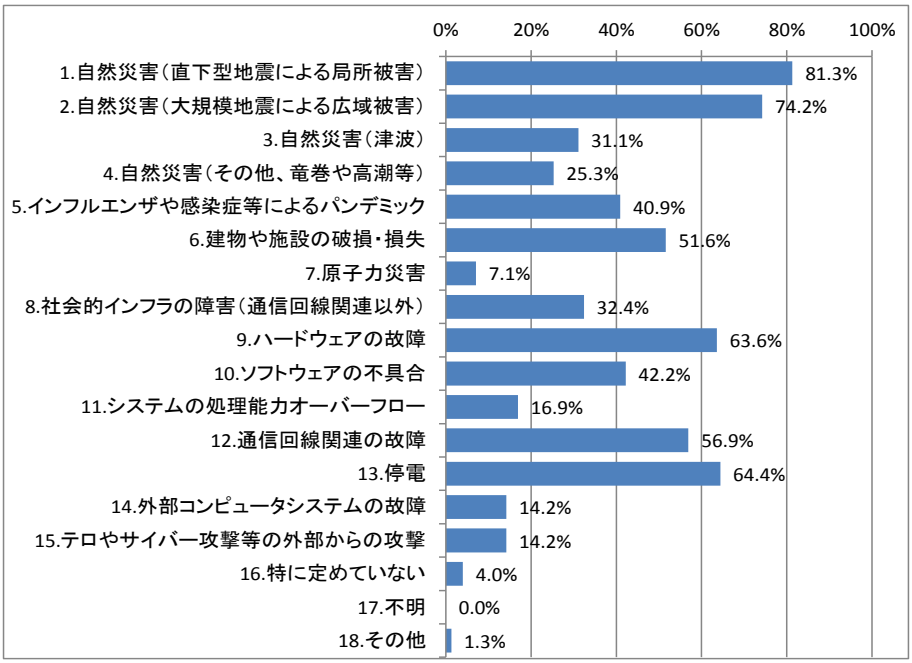


図 4-8 IT サービス継続計画策定時に想定するリスク（n=225）

表 4-3 [業種別] IT サービス計画策定時に想定するリスク（n=225）

	建設業	製造業	卸売・小売業、飲食店	金融・保険業	不動産業	運輸・通信業	電気・ガス・水道・熱供給業	サービス業	その他	全業種平均
1. 自然災害（直下型地震による局所被害）	67%	73%	88%	71%	80%	95%	－	86%	100%	81%
2. 自然災害（大規模地震による広域被害）	67%	67%	76%	79%	70%	64%	－	86%	100%	74%
3. 自然災害（津波）	33%	29%	32%	36%	30%	23%	－	34%	50%	31%
4. 自然災害（その他、竜巻や高潮等）	33%	23%	29%	21%	10%	23%	－	30%	50%	25%
5. インフルエンザや感染症等によるパンデミック	33%	37%	41%	64%	10%	32%	－	50%	－	41%
6. 建物や施設の破損・損失	33%	48%	65%	57%	30%	64%	－	50%	－	52%
7. 原子力災害	－	5%	3%	7%	－	9%	－	13%	－	7%
8. 社会的インフラの障害（通信回線関連以外）	－	28%	44%	29%	20%	36%	－	36%	－	32%
9. ハードウェアの故障	33%	67%	62%	71%	50%	59%	－	67%	－	64%
10. ソフトウェアの不具合	67%	39%	41%	57%	50%	32%	－	47%	－	42%
11. システムの処理能力オーバーフロー	－	9%	12%	21%	20%	14%	－	30%	－	17%
12. 通信回線関連の故障	33%	52%	59%	57%	40%	45%	－	70%	50%	57%
13. 停電	－	68%	76%	43%	50%	59%	－	67%	50%	64%
14. 外部コンピュータシステムの故障	－	9%	18%	29%	10%	14%	－	17%	－	14%

	建設業	製造業	卸売・小売業、飲食店	金融・保険業	不動産業	運輸・通信業	電気・ガス・水道・熱供給業	サービス業	その他	全業種平均
15. テロやサイバー攻撃等の外部からの攻撃	33%	11%	12%	29%	－	5%	－	22%	－	14%
16. 特に定めていない	－	8%	－	－	－	－	100%	－	－	4%
17. その他	－	－	－	7%	－	－	－	3%	－	1%

※各業界で上位から 2 位となったリスクを網掛け

また、企業が想定するリスクの対象件数をみると、各企業は平均して 6.2 件のリスクを想定していた。業種別では、サービス業や金融・保険業、卸売・小売、飲食店が、平均を上回る件数のリスクを挙げていることから、他の業種の企業と比較して多様なリスクを想定する傾向にあることがうかがえる（図 4-9）。

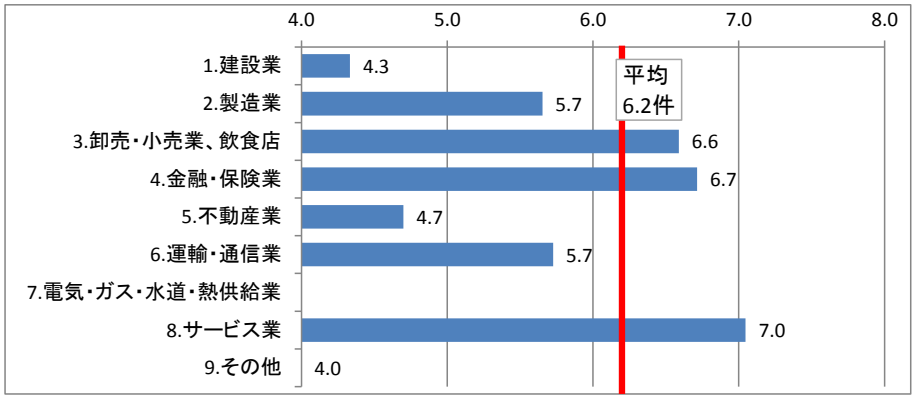


図 4-9　業界別の 1 社あたりのリスク列挙件数（n=217）

IT サービス継続に関して重点的に取り組んでいる領域は、上位 3 件に「冗長化された電源供給やネットワーク」、「データの遠隔地保管」、「情報処理設備や機器の冗長化」が挙げられている（図 4-10）。インフラ面では電源やネットワークが、情報システム面ではハードウェアの冗長化とデータの遠隔地保管を重視している企業が多い。

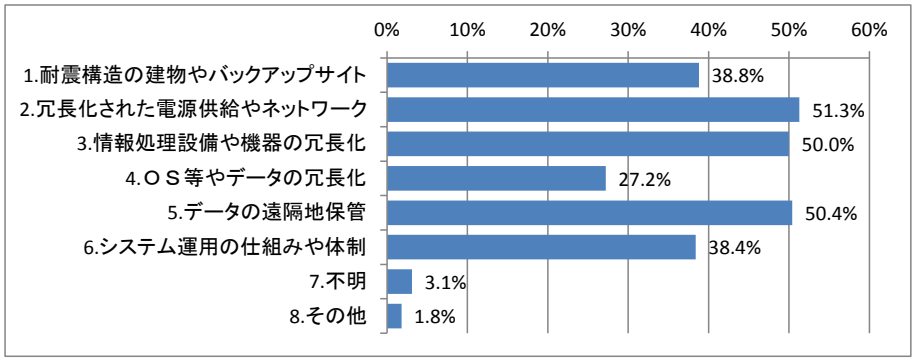


図 4-10　重点的に取り組んでいる領域（n=224）

② コンピュータシステムと新しい技術の採用状況

事業継続における最も影響の大きいシステムについて、対象のシステムとその構成、仮想化技術とクラウドサービスの採用状況に関する調査を行った。

a. 重要システムとバックアップ対象

「事業継続において最も重要なシステム(重要システム)」をたずねたところ、「財務・会計管理システム」が65%と最も多く、次いで「販売管理システム」が43%、「メール・グループウェア」が29%となった。これらを業種毎に集計すると、製造業が「生産管理システム」を、金融・保険業では「勘定系システム」を多く挙げるなど、業種の特徴により異なる傾向があった(表 4-4)。

表 4-4 [業種別] 事業継続において最も重要なシステム(n=357)

	建設業	製造業	卸売・小売業、飲食店	金融・保険業	不動産業	運輸・通信業	電気・ガス・水道・熱供給業	サービス業	その他	全業種平均
1. 財務・会計管理システム	92%	60%	74%	56%	89%	64%	50%	61%	40%	65%
2. 人事管理システム	38%	15%	19%	6%	16%	27%	−	22%	20%	19%
3. 販売管理システム	23%	58%	82%	22%	11%	21%	25%	21%	40%	43%
4. 生産管理システム	23%	69%	11%	−	−	−	25%	8%	−	27%
5. 物流・在庫管理システム	−	47%	48%	−	−	21%	−	4%	20%	27%
6. 勘定系システム	8%	12%	16%	39%	5%	6%	25%	9%	−	12%
7. 開発管理システム	−	7%	−	6%	−	3%	−	16%	−	7%
8. 設備管理システム	−	−	−	6%	−	12%	25%	4%	−	3%
9. 企業間連携システム	8%	4%	6%	11%	−	9%	25%	6%	−	6%
10. Web 上の個人向けサービス提供システムや販売サイトのシステム(SNS、ショッピングサイト等)	−	−	11%	6%	5%	9%	−	14%	−	7%
11. 顧客管理システム	23%	8%	23%	33%	21%	24%	25%	23%	20%	19%
12. 分析系システム (BI/DWH)	−	4%	6%	6%	−	−	−	2%	−	3%
13. 営業支援システム (SFA)	15%	3%	8%	6%	−	−	−	7%	−	5%
14. メール・グループウェア	15%	27%	32%	17%	16%	33%	−	37%	40%	29%
15. 社内向けホームページ	8%	1%	5%	6%	5%	−	−	2%	−	3%
16. 社外向けホームページ	−	4%	10%	11%	5%	15%	−	19%	40%	11%
17. 運用・セキュリティ関連システム	8%	3%	3%	17%	−	9%	−	17%	40%	8%
18. その他	15%	2%	−	22%	5%	18%	−	14%	40%	8%

※各業種別に上位 2 位のシステムを網掛け(ただし第 2 位が複数ある場合は網掛けせず)

データの保管対象となるシステム(バックアップ対象システム)をたずねたところ、重要システムと同様のシステムが選択される傾向はあるものの、一部に異なる傾向が見られた。たとえば、「メール・グループウェア」は重要システムとして上から3番目となっており、「生産管理システム」や「物流・在庫管理システム」、「人事管理システム」よりも高い割合で挙げられている。しかし、バックアップ対象システムとして「メール・グループウェア」の位置づけはそれらのシステムよりも低くなっている。また、「人事管理システム」や「販売管理システム」は、バックアップ対象システムの割合が重要システムの割合を

上回っている点などが挙げられる(図 4-11)。このことから、事業継続において重要なシステムと、データの保管がなされているシステムは必ずしも一致しないことが分かった。

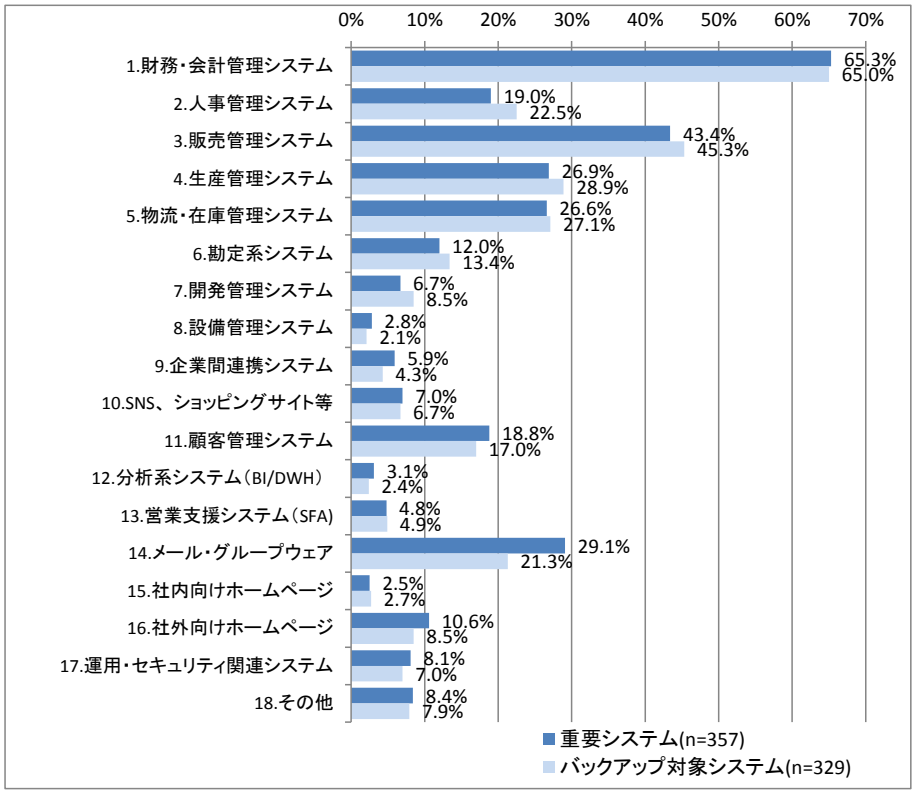


図 4-11 事業継続において最も重要なシステムとバックアップ対象システム

b. 仮想化技術やクラウドサービスの利用状況

仮想化技術を「利用している」と「利用していない(検討中)」を合わせて 48.7%となっている(図 4-12 左)。また、クラウドサービスを「利用している」と「利用していない(検討中)」を合わせて 40.2%となっている(図 4-12 右)。事業継続に最も重要なシステムにおいては、半数近くの企業が仮想化やクラウドの採用に前向きな姿勢を見せている一方、半数の企業は消極的である。

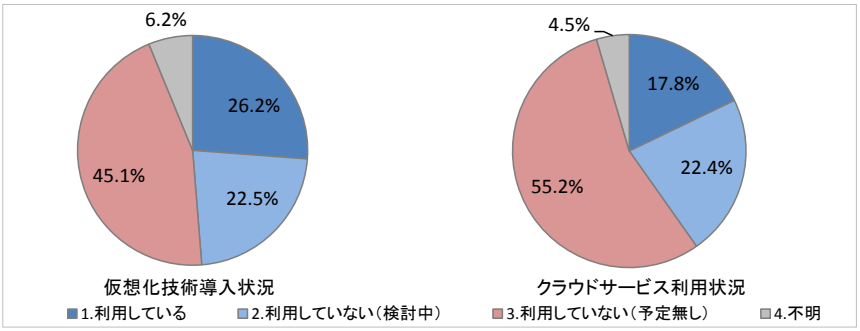


図 4-12 左:仮想化技術導入状況(n=355)／右:クラウドサービス利用状況(n=353)

クラウドサービスを円滑に導入するためには、システムへの仮想化技術の導入が有効だと言われている。クラウドサービスが仮想化技術によって構成されているためである。そこで、クラウドサービスの利用者別の仮想化技術導入状況を確認したところ、仮想化技術の導入とクラウドサービスの利用には相関があることが確認できた。クラウドサービス利用者の仮想化技術導入率が 54.0%である一方、クラウドサービス未利用者の仮想化技術導入率が 21.2%となっている(図 4-13)。このことから、クラウドサービスを利用している企業は、既存環境の仮想化も合わせて進めているケースが多いことが推察される。クラウドサービスの導入を検討する企業においては、まずは仮想化技術の導入から検討することも一つの方法だと考えられる。

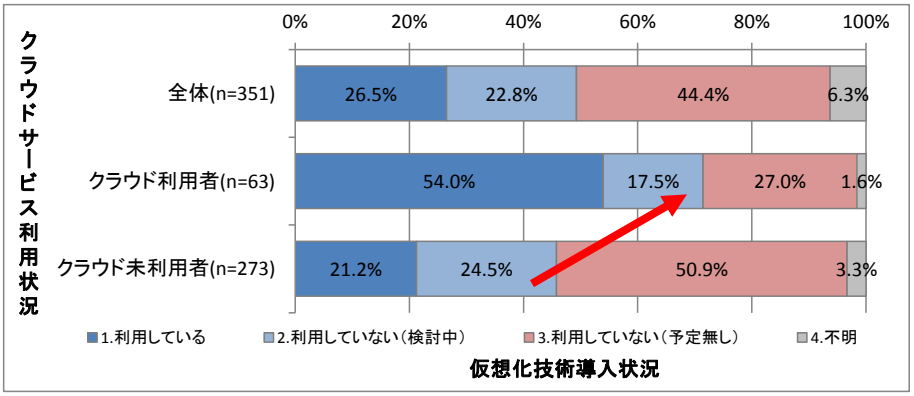


図 4-13 [クラウドサービス利用状況別] 仮想化技術導入状況

利用中のクラウドサービスは、SaaS 型のサービスが 65.1%と最も多い。一方、それ以外の PaaS、IaaS 等は利用の割合が少ない(図 4-14)。3.1.3 で紹介している遠隔バックアップサービスやデータセンタ/クラウドの付加機能は、PaaS や IaaS に該当するが、企業の復旧能力の向上に向け、これらのサービスの普及が期待される。

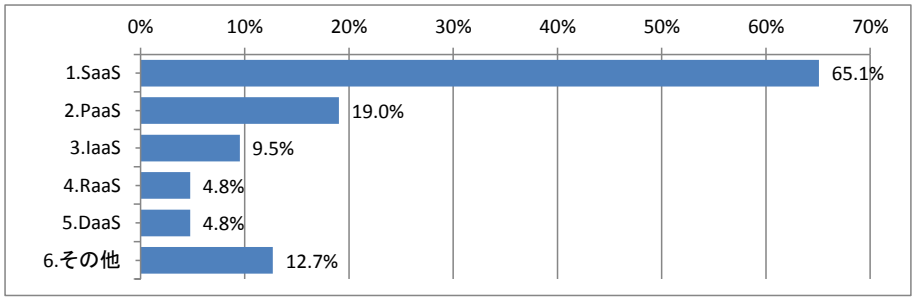


図 4-14 利用中のクラウドサービス(n=63)

クラウドサービスの導入目的は、「利用中」の企業では「運用・保守費用の低減」が筆頭となっており、「利用していない(検討中)」企業では「災害への対策」が筆頭となっている。また、利用中企業と検討中企業との間で上位 3 つの項目は同様であるものの、順番が異なることから、期待と実際が異な

っていることがうかがえる(「利用中」企業は、「運用・保守費用の低減」、「導入費用の低減」、「災害対策への対策」の順になっている。「利用していない(検討中)」の企業は「災害への対策」、「運用・保守費用の低減」、「導入費用の低減」の順となっている。)(図 4-15)。

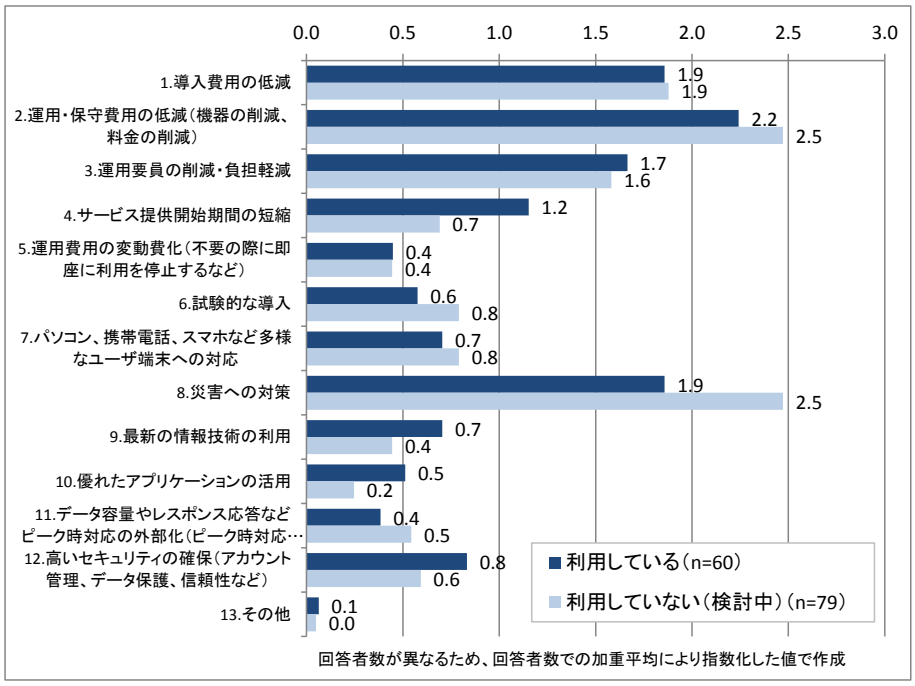


図 4-15 [クラウドサービスの利用状況別] クラウドサービスの導入目的

③ システム構成

事業継続において最も影響の大きいシステムの構成について、システム構成や冗長化の状況に関する調査を行った。

a. システムの冗長化の状況

事業継続において最も影響の大きいシステムの冗長化の状況をたずねたところ、待機系システムが設置されているシステムは 52.8%となった。そのうち、遠隔にも待機系システムが設置されているのは 15.3%となっている(図 4-16)。待機系システムの設置は、IT サービスの可用性や復旧能力を向上させるための有効な対策の一つではあるものの、費用を理由に導入に踏み切れないという声が聞かれる。事業の IT 依存度別に待機系システムの設置状況を見ると、IT 依存度が高いほど待機系システムを設置している傾向が強い。システムの冗長化は、多くの費用が掛かる対策ではあるものの、事業や業務への影響を考慮して待機系システムを設置していることがうかがえる。

また、資本金や拠点数、従業員数の規模が大きくなるにしたがい、待機系システムを設置している傾向が強くなっている。事業規模が大きくなれば、IT 投資予算も大きくなる傾向が想定され、それによって IT 依存度が高まり、結果的に待機系システムを設置する必要性が高まっていると考えられる。

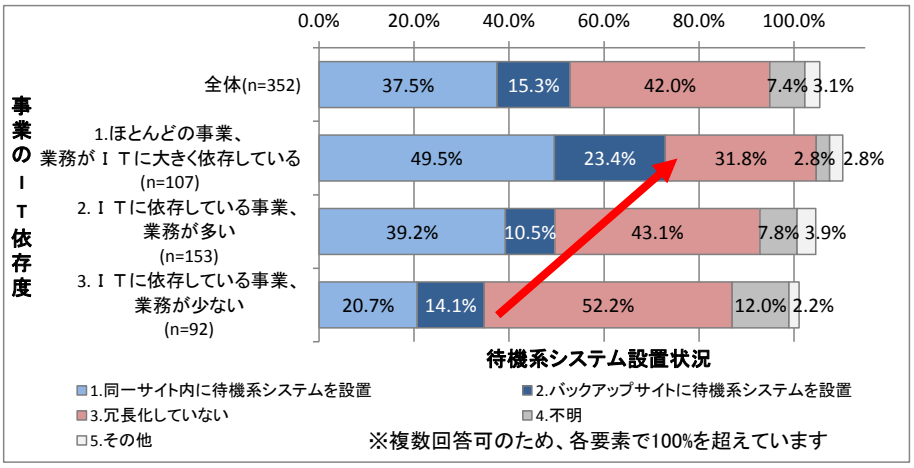


図 4-16 [事業の IT 依存度別] システム(サーバ)の冗長化の状況

業種別に見た場合、金融・保険業の待機系システムを設置している割合が 83.3%と最も高い(同一サイトとバックアップサイトの延べ数で算出)。金融・保険業は IT 依存度が最も高い業種である(「ほとんどの事業、業務が IT に依存している」と「IT に依存している事業、業務が多い」を合わせて 88.3%)ことからも、IT 依存度の高さと待機系システム設置割合の相関を確認することができる(図 4-17)。

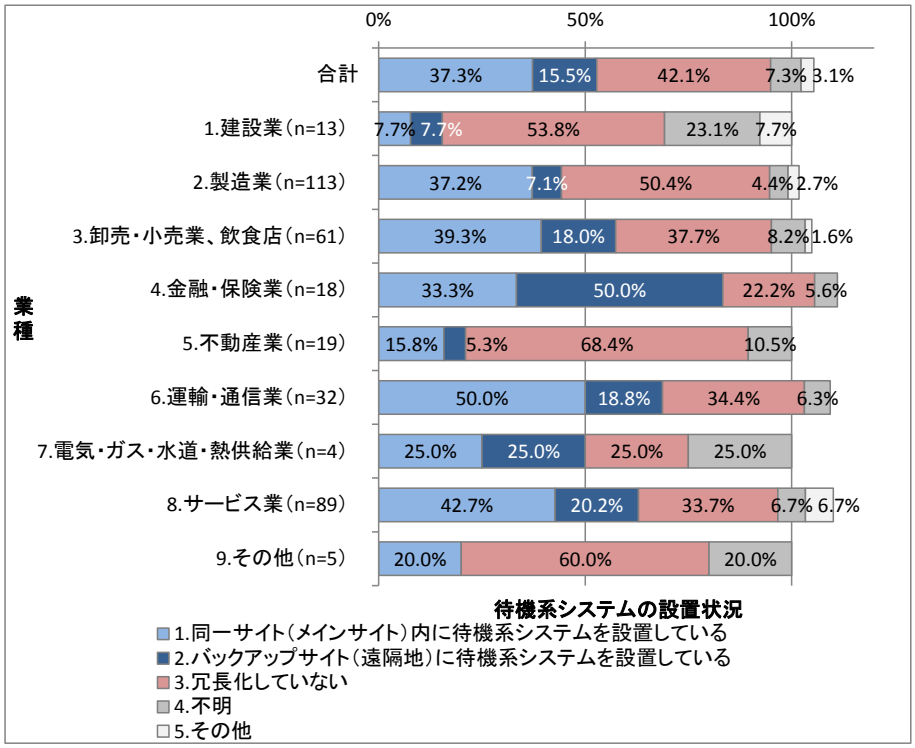


図 4-17 [業種別] 待機系システムの設置状況

④ リカバリ要件定義の有無

リカバリ要件定義の有無について、事業継続に最も影響の大きいシステムの目標復旧時間（RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）といったサービス継続の復旧目標の設定状況に関する調査を行った。

a. リカバリ要件定義の有無

事業継続に最も影響の大きいシステムの目標復旧時間（RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）を策定している企業は 2 割程度にとどまっており、各指標とも同様の傾向となっている（図 4-18）。

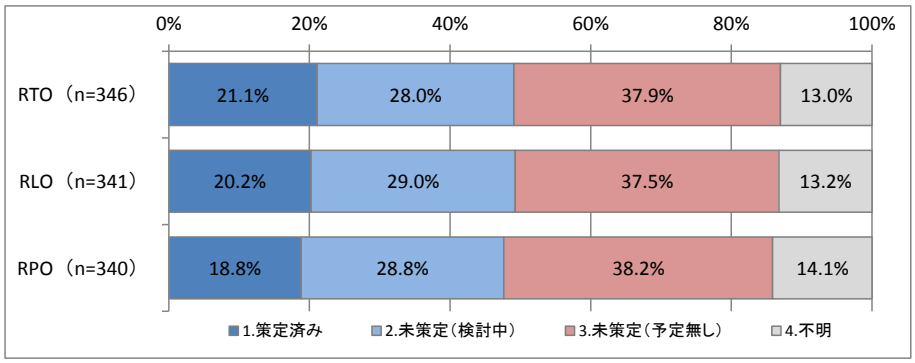


図 4-18　目標復旧時間（RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）

BCP や IT-BCP の策定状況との相関を見ると、計画を策定している企業ほど、リカバリ要件定義を策定している割合が高い（図 4-19、図 4-20）。また、事業の IT 依存度の高さ別に見ると、IT 依存度が高いとする企業ほどリカバリ要件定義を設定している割合が高い（図 4-21）。このことから、BCP や IT-BCP が策定されていたり、IT 依存度の高さを認識していたりする企業ほど、復旧に対する具体的な目標に基づき対策を実施していることが推察される。

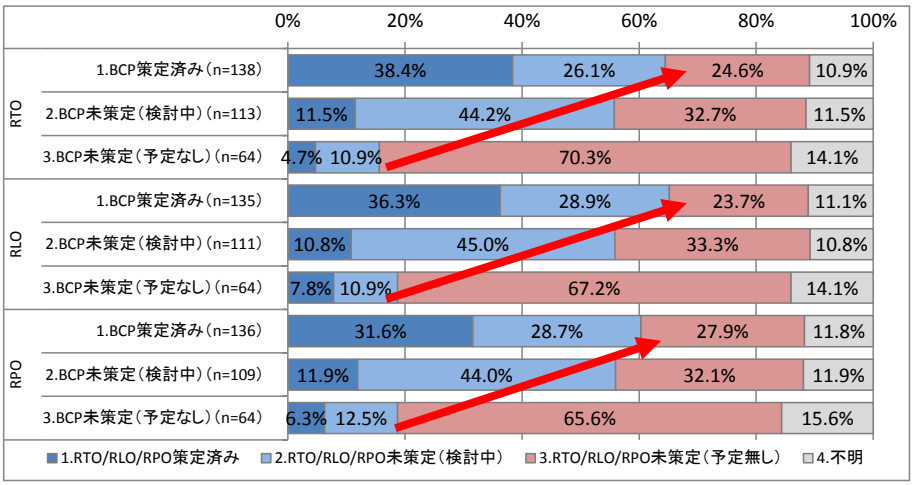


図 4-19 [BCP 策定状況別] 目標復旧時間（RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）

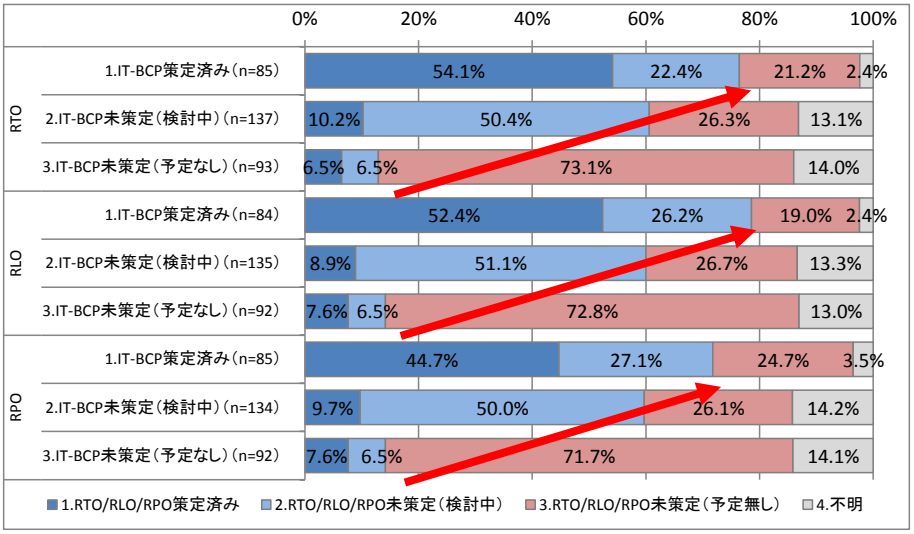


図 4-20 [IT-BCP 策定状況別] 目標復旧時間（RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）

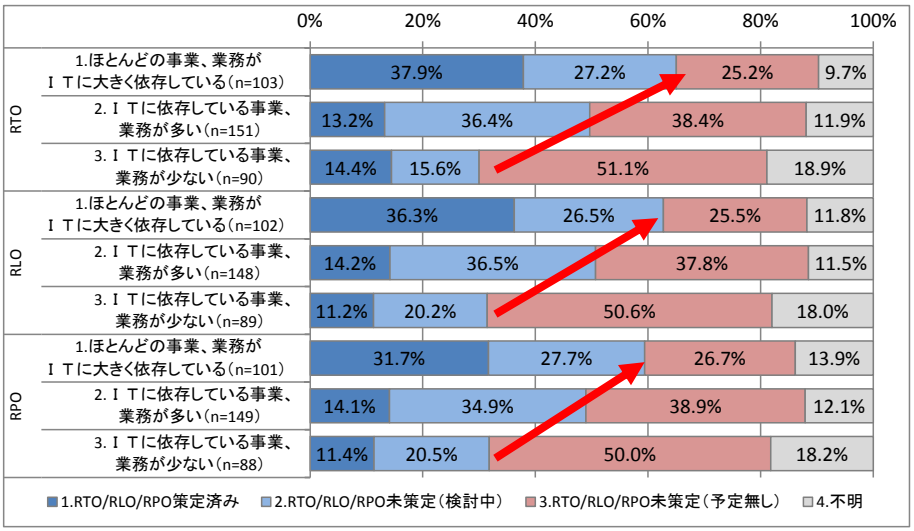


図 4-21 [事業の IT 依存度の高さ別] 目標復旧時間（RTO）、目標復旧レベル（RLO）、目標復旧時点（RPO）

IT-BCP を「策定済み」および「未策定（検討中）」とした企業に、IT サービス継続に関する取り組み状況をたずねており、それらの取り組み状況と事業継続に最も影響の大きいシステムに対する目標復旧時間の関係を集計した。それによると、IT サービス継続における各取り組みを実施している企業の方が、目標復旧時間（RTO）を「策定済み」としている割合が高い（図 4-22）。一般的に、共通の目標は、複数の関係者同士が協力して取り組みを推進する場合に重要な役割を果たすことから、複数部門が関連する IT サービス継続の取り組みにおいては、目標復旧時間（RTO）等の具体的な指標が、重要な役割を果たしていると推察される。

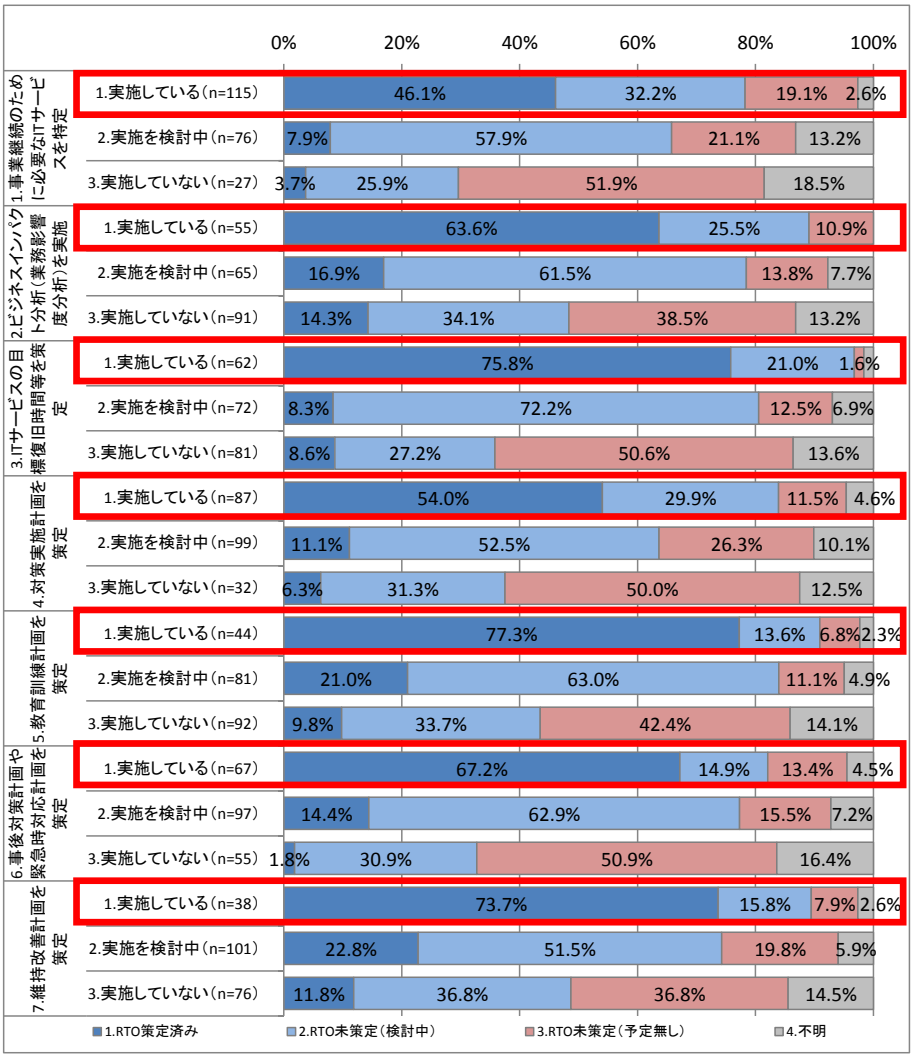


図 4-22 [IT サービス継続への取り組み状況別] 事業継続に最も影響の大きいシステムの目標復旧時間(RTO)の策定状況

目標復旧時間(RTO)は、「1 時間～6 時間未満」が 28.0%と最も多い(図 4-23)。目標復旧レベル(RLO)は、「障害・被災前と同等の業務を実施できる水準」が 42.1%と最も多い(図 4-24)。目標復旧時点(RPO)は、「障害・被災発生の前日まで復旧」が 48.1%と最も多い(図 4-25)。

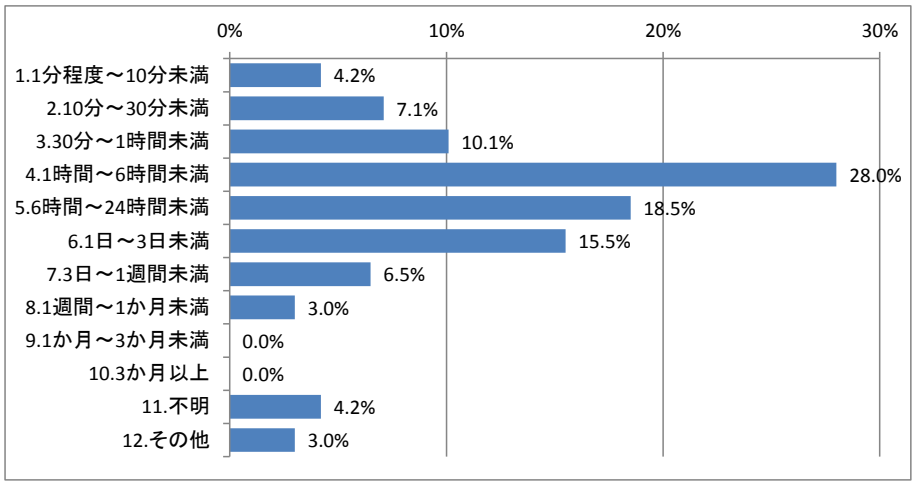


図 4-23　目標復旧時間（RTO）（n=168）

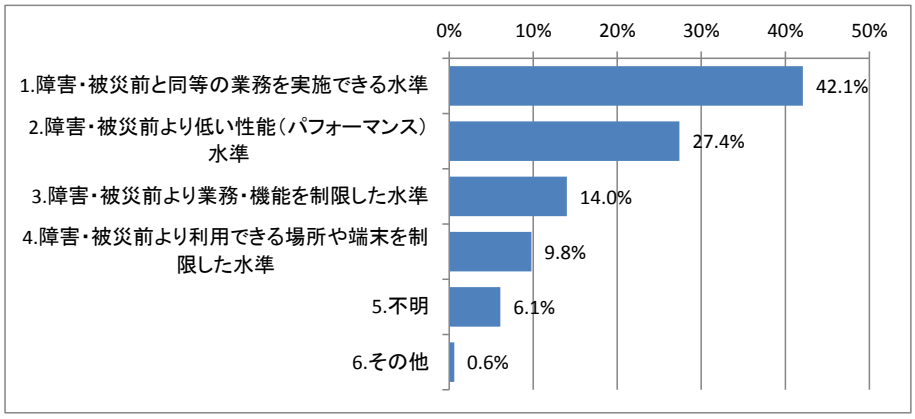


図 4-24　目標復旧レベル（RLO）（n=164）

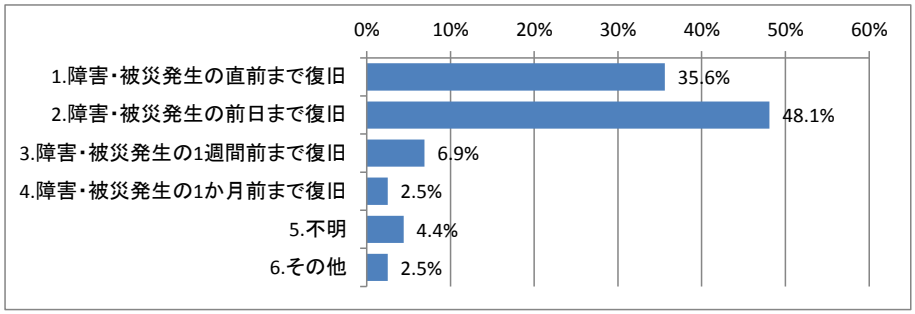


図 4-25　目標復旧時点（RPO）（n=160）

リカバリ要件定義とシステム復旧対策の整合状況を確認するため、目標復旧時間（RTO）とシステム冗長化の状況を集計した。図 4-26 のとおり、目標復旧時間（RTO）毎に企業をグルーピングし、それぞれのシステム冗長化状況を確認したところ、目標復旧時間（RTO）が 6 時間未満のグループであ

っても、システムの冗長化を行っていない企業が、各グループで15%～25%程度あった。システムが冗長化されていない状態では、大規模障害や大規模災害に直面した場合、想定通りの対応（6 時間未満での復旧）を実現できる可能性は低いと思われる。事業継続性を確保するためには、IT サービス継続戦略と対策の整合性を確保しておくことが重要である。

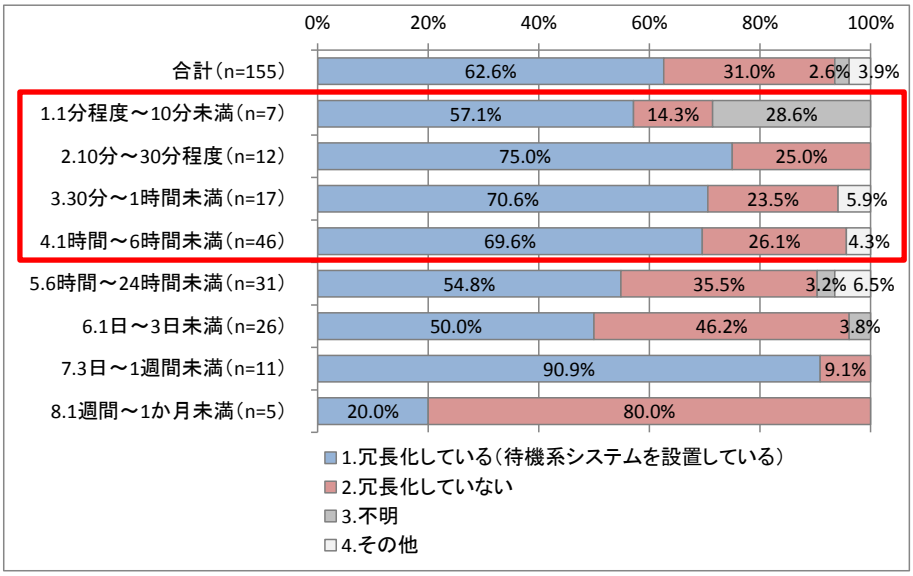


図 4-26 [RTO 別] システム冗長化の状況

⑤ データの保管（バックアップ）の実施状況

事業継続において最も影響の大きいシステムの、データ保管（バックアップ）の実施状況について、バックアップポリシーの明確化状況、バックアップ対象、実行単位、取得期間、保管場所の分散度等に関する調査を行った。

a. バックアップ及びバックアップポリシーの整備状況

92.7%の企業がデータの保管（バックアップ）を実施している。少数であるが、データの保管を実施していない企業が 5.0%あった（図 4-27）。データの保管を実施していない企業の半数は、「IT に依存している事業、業務が少ない」と回答している。一方で残りの半数は「ほとんどの事業、業務が IT に大きく依存している」または「IT に依存している事業、業務が多い」と回答している。データの保管は、大規模災害や大規模システム障害からの復旧対策として有効だと考えられている取り組みの一つであるが、IT への依存度が高く、対策の必要性の高い企業であっても実施されていない例がある。

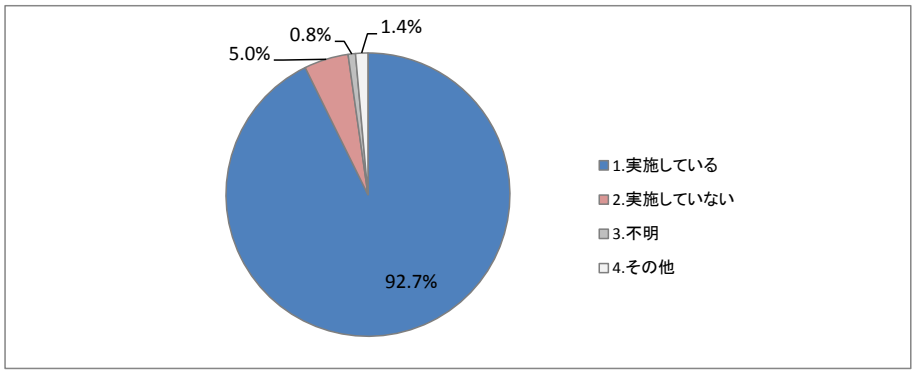


図 4-27 データの保管（バックアップ）の実施状況（n=357）

バックアップを実施している企業のうち、「全社的にガイドラインを定めており、全部または一部のシステム毎に明確化している」または「全社的にガイドラインを定めているが、個別のシステムのバックアップポリシーには反映していない」と回答した企業は 33.1%となっている。また、これらの企業を含め 71.0%の企業が何らかの形でバックアップポリシーを明確化している（図 4-28）。

一方、26.1%はバックアップポリシーを明確にしていないことから、これらの企業は成行きでバックアップデータを保管している可能性が考えられる。これらの企業のうち 59.3%は IT 依存度が高い（「ほとんどの事業、業務が IT に大きく依存している」または「IT に依存している事業、業務が多い」）としている（図 4-29）。IT 依存度が高いにも関わらず、バックアップポリシーが明確化されていない場合、適切な復旧目標を検討できない可能性が考えられる。バックアップポリシー明確化の有効性についての認知度を向上させる取り組みは、社会的な復旧能力を向上させる上でも重要な取り組みになると考えられる。

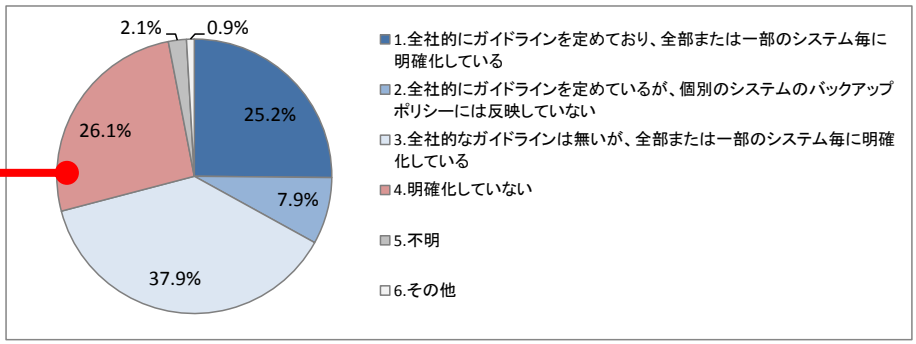


図 4-28　バックアップポリシーの明確化（n=330）

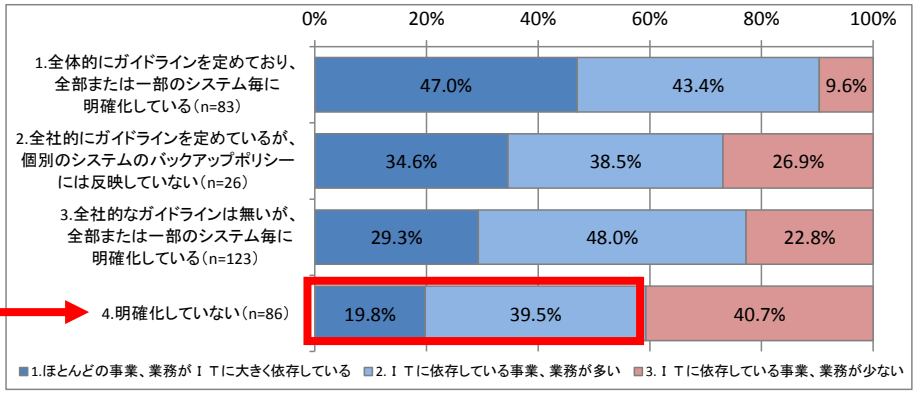


図 4-29 ［バックアップポリシー明確化状況別］業務の IT 依存度

b. バックアップの実施状況

データの保管を実施している企業のうち、「データ（データベース関連のデータ）」をバックアップ対象としている企業が 94.2%と最も多い（図 4-30）。また、バックアップ実行単位の観点では、「バックアップ対象毎に別々にバックアップ」が 72.0%と最も多い（図 4-31）。多くの企業で複数種類のデータをバックアップ対象とし、複数の方法でバックアップを実施しているものの、企業等の認識の変化や技術の進展により、これまで以上に多様化される余地があると考えられる。3.1 において復旧に有効な技術やサービスとして仮想化技術やクラウドサービスを取り上げているが、これらの技術やサービスの普及が進むことにより、バックアップ対象の拡大や、状況に合わせたバックアップ方法の選択が容易になることが期待される。

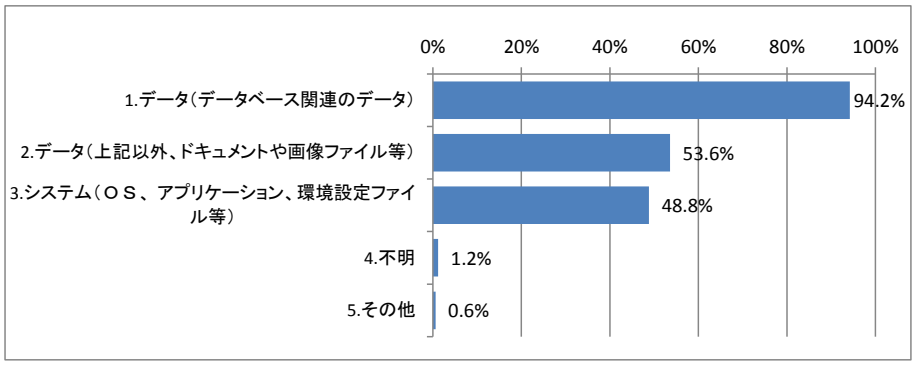


図 4-30　バックアップ対象（n=330）

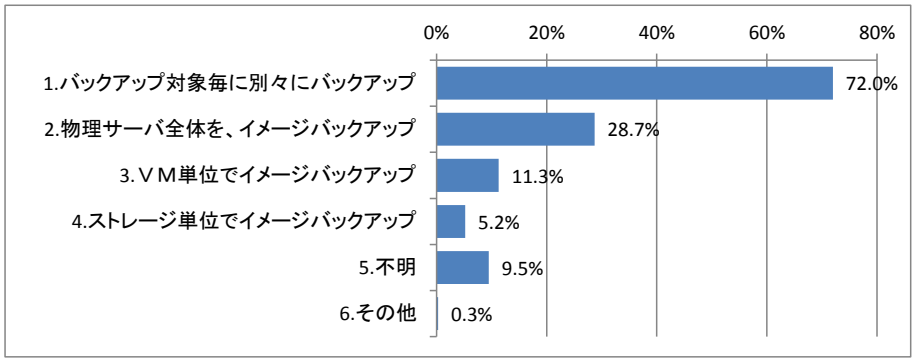


図 4-31　バックアップの実行単位（n=328）

バックアップデータは、36.1%が「別拠点へのバックアップあり」としており、52.9%が「同一の拠点のみでバックアップ」となっている（図 4-32）。2.1 で示した企業等における動向や本アンケート調査において、これから見直す対策に、バックアップデータの保管場所の分散度が挙げられていることから、今後別拠点に保管する企業が増加することが予想される。

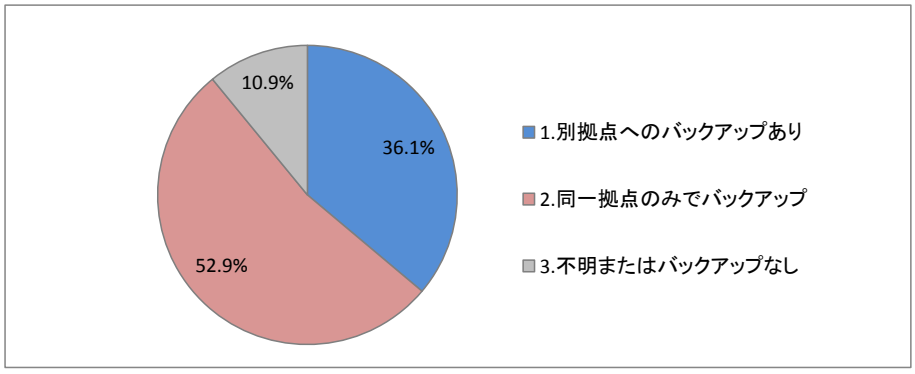


図 4-32　バックアップの保管場所の分散度（n=357）

バックアップの実施状況について、資本金規模別、事業の IT 依存度別の 2 つの分析軸に沿って、

それぞれの傾向を確認した(表 4-5、表 4-6)。概ね資本金規模や IT 依存度が大きくなればデータの保管対策は充実する傾向にある(図 4-33、図 4-34、図 4-35、図 4-36)。事業規模が大きくなるにしたがい、事業におけるITの位置づけが大きくなり、結果的にデータの保管対策が充実していることが推察される。

しかし、IT 依存度別のバックアップの保管場所の分散度を確認すると、「ほとんどの事業、業務が IT に大きく依存している」企業であっても、「別拠点(本番システムが設置されている拠点との距離が 60Km 以上)」が 32.0%、「別拠点(本番システムが設置されている拠点との距離が 60Km 未満)」が 17.5%にとどまっており(表 4-6、図 4-36)、多くの企業で東日本大震災級の大災害には十分に対応できない可能性がある。IT 依存度が高く、十分な対策を実施している企業であっても、改めて対策の見直しが必要だと考えられる。

表 4-5 [資本金規模別] データの保管(バックアップ)の傾向

設問項目	資本金規模別の特徴
バックアップポリシーの明確化	・資本金規模が大きいほど、バックアップポリシーを明確化している傾向が強い
バックアップ対象	・「データ(データベース関連データ)」と「データ(ドキュメントや画像ファイル等)」では、資本金規模別の違いは見られないが、「システム(OS、アプリケーション、環境設定ファイル等)」は資本金規模が大きくなるにしたがい、バックアップ対象とする割合が高い
バックアップの実行単位	・資本金規模が大きいほど、バックアップの実行単位が多様化している
データの完全性	・100 億円以上の企業は「データの完全性や復旧時のエラー検出に関する要件を定めている」割合が他の区分よりも高い
バックアップの方式	・100 億円以上の企業は、オフラインバックアップを採用している傾向が強い ・資本金規模が大きいほど、オンラインバックアップとオフラインバックアップを組み合わせている傾向が強い
バックアップの頻度	・資本金規模が大きいほど、バックアップの頻度が多様化している ・資本金規模が大きいほど、リアルタイムバックアップを行っている傾向が強い
バックアップの世代管理	−
バックアップしている媒体	・資本金規模が大きいほど、「磁気テープ」の割合が増える ・資本金規模が大きいほど、「外付けハードディスクドライブ」の利用が減少し、「ストレージ装置」の利用が増加している
バックアップの保管場所の分散度	・資本金規模が大きいほど、別拠点に保管する割合が高くなり、本番システムが設置されている拠点との距離も離れる傾向が強い
異なる拠点でのバックアップデータの取得間隔	・資本金規模が大きいほど、バックアップデータの取得間隔が多様化している ・100 億円以上の企業は、「リアルタイム」と「非同期(日次)」の割合が増加している
バックアップデータの施錠管理状況	・資本金規模が大きいほど、施錠対象が増加する傾向が強い ・資本金規模が大きいほど、「外部のデータ保管サービスを利用している」割合が増加している
バックアップデータの暗号化	・資本金規模が大きいほど、バックアップデータを暗号化する企業が増加する傾向が強い
バックアップ作業の自動化の範囲	・資本金規模が大きいほど、バックアップを手動で行う割合が減少している

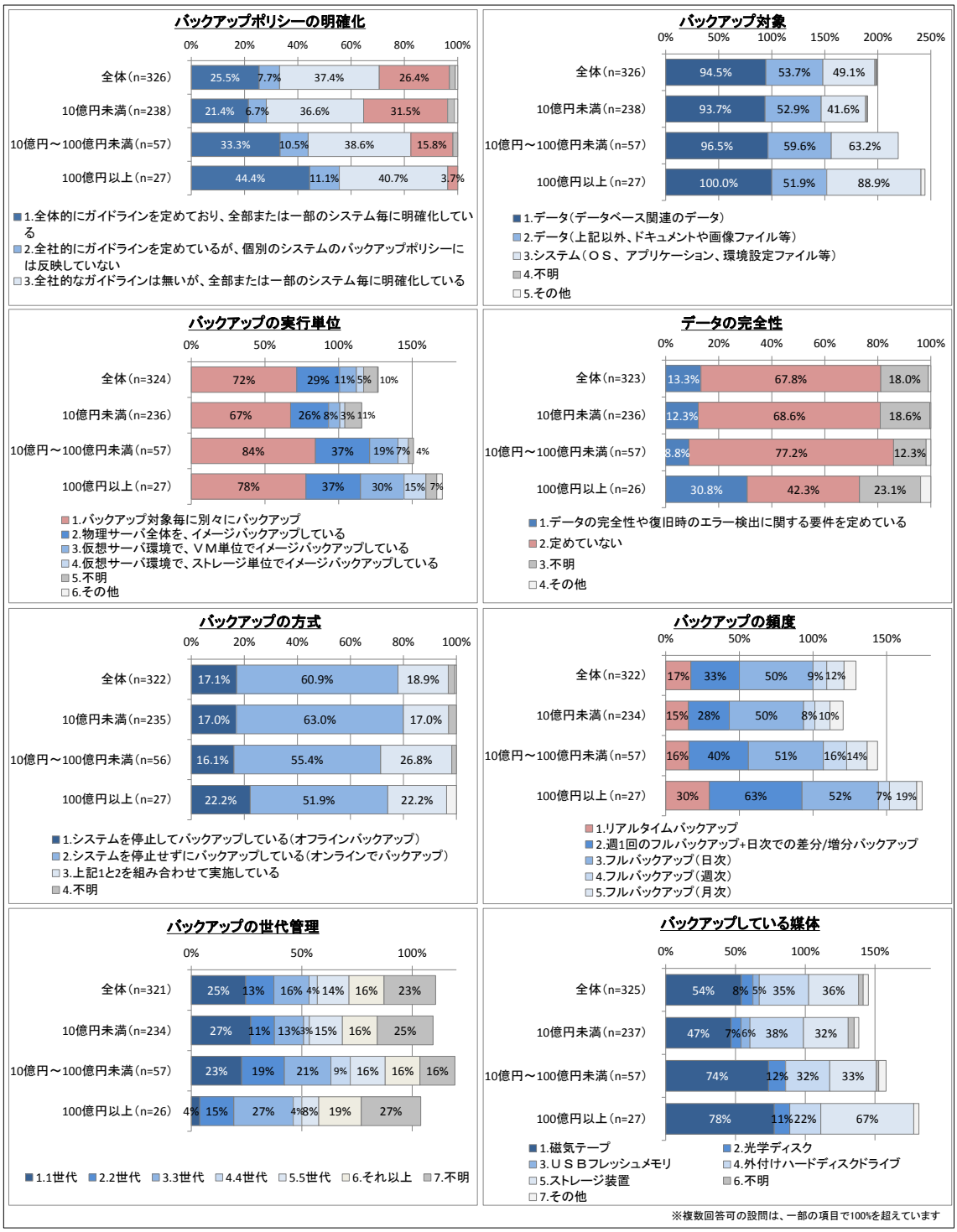


図 4-33 [資本金規模別] データの保管（バックアップ）実施状況（1/2）

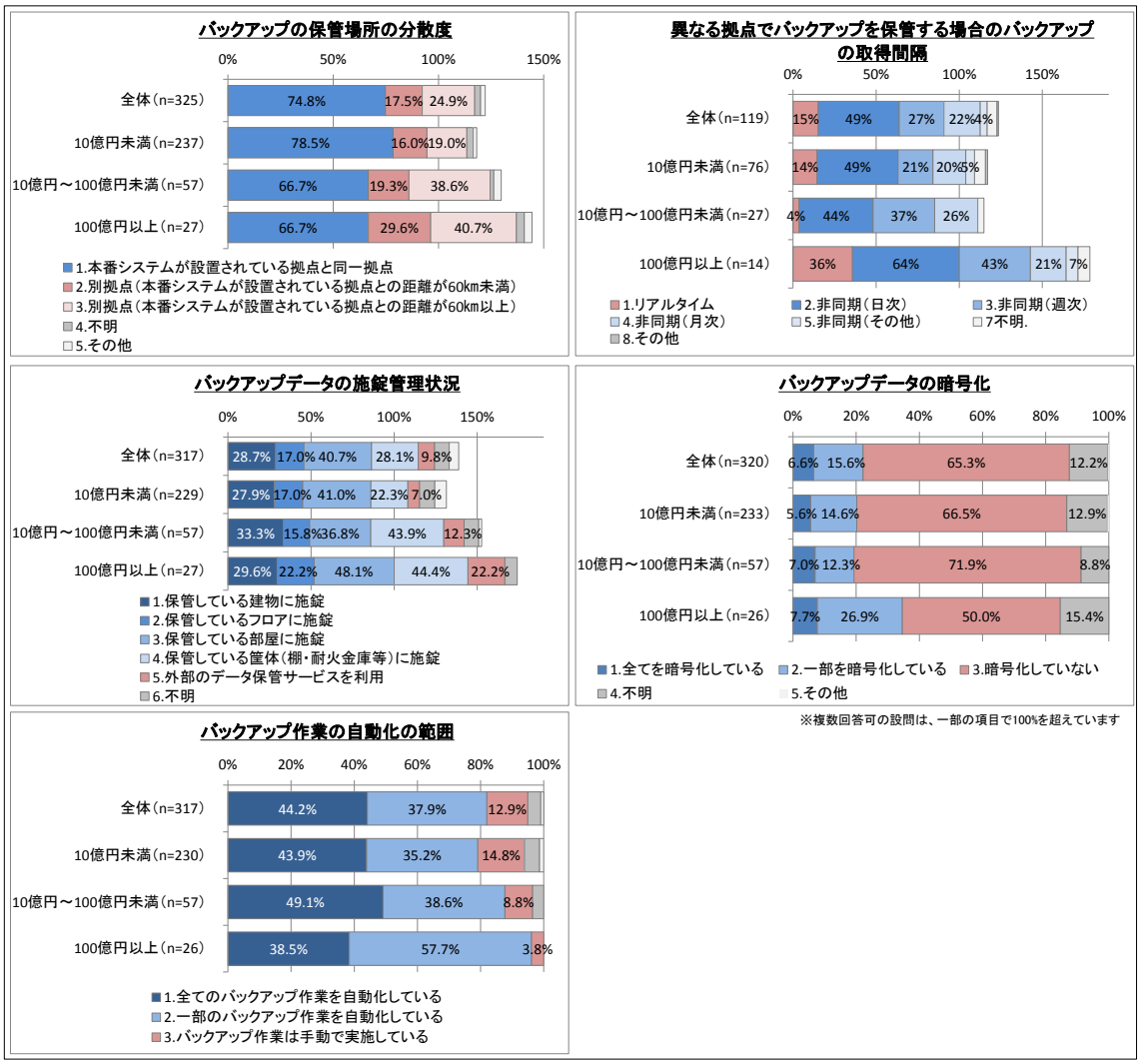


図 4-34 [資本金規模別] データの保管(バックアップ)実施状況(2/2)

表 4-6 [事業の IT 依存度別] データの保管(バックアップ)の傾向

設問項目	事業の IT 依存度別の特徴
バックアップポリシーの明確化	・IT 依存度が高いほど、バックアップポリシーを明確化している傾向が強い
バックアップ対象	・「データ(データベース関連データ)」と「データ(ドキュメントや画像ファイル等)」では、IT 依存度別の違いは見られないが、「システム(OS、アプリケーション、環境設定ファイル等)」は IT 依存度が高いほど、バックアップ対象とする傾向が強い
バックアップの実行単位	・IT 依存度が高いほど、バックアップの実行単位が多様化している
データの完全性	・IT 依存度が高いほど、「データの完全性や復旧時のエラー検出に関する要件を定めている」傾向が強い
バックアップの方式	・IT 依存度が高いほど、オンラインバックアップとオフラインバックアップを組み合わせている傾向が強い
バックアップの頻度	・IT 依存度が高いほど、バックアップの頻度が多様化している ・IT 依存度が高いほど、リアルタイムバックアップを行っている傾向が強い
バックアップの世代管理	・IT 依存度が高いほど、複数世代でのバックアップを行っている傾向が強い
バックアップしている媒体	・IT 依存度が高いほど、「磁気テープ」の割合が増える ・IT 依存度が高いほど、「外付けハードディスクドライブ」の利用が減少し、「ストレージ装置」の利用が増加している
バックアップの保管場所の分散度	・「ほとんどの事業、業務が IT に大きく依存している」企業は、「本番システムが設置されている拠点(60Km 以上)」に保管する割合が高いものの、32.0%にとどまる
異なる拠点でのバックアップデータの取得間隔	・IT 依存度が高いほど、バックアップデータの取得間隔が多様化し、取得間隔が短くなっている
バックアップデータの施錠管理状況	・IT 依存度が高いほど、施錠対象が増加する傾向が強い ・IT 依存度が高いほど、「外部のデータ保管サービスを利用している」割合が増加している
バックアップデータの暗号化	・IT 依存度が高いほど、バックアップデータを暗号化する企業が増加する傾向が強い
バックアップ作業の自動化の範囲	・IT 依存度が高いほど、バックアップ作業を自動化する割合が増加し、バックアップを手動で行う割合が減少している

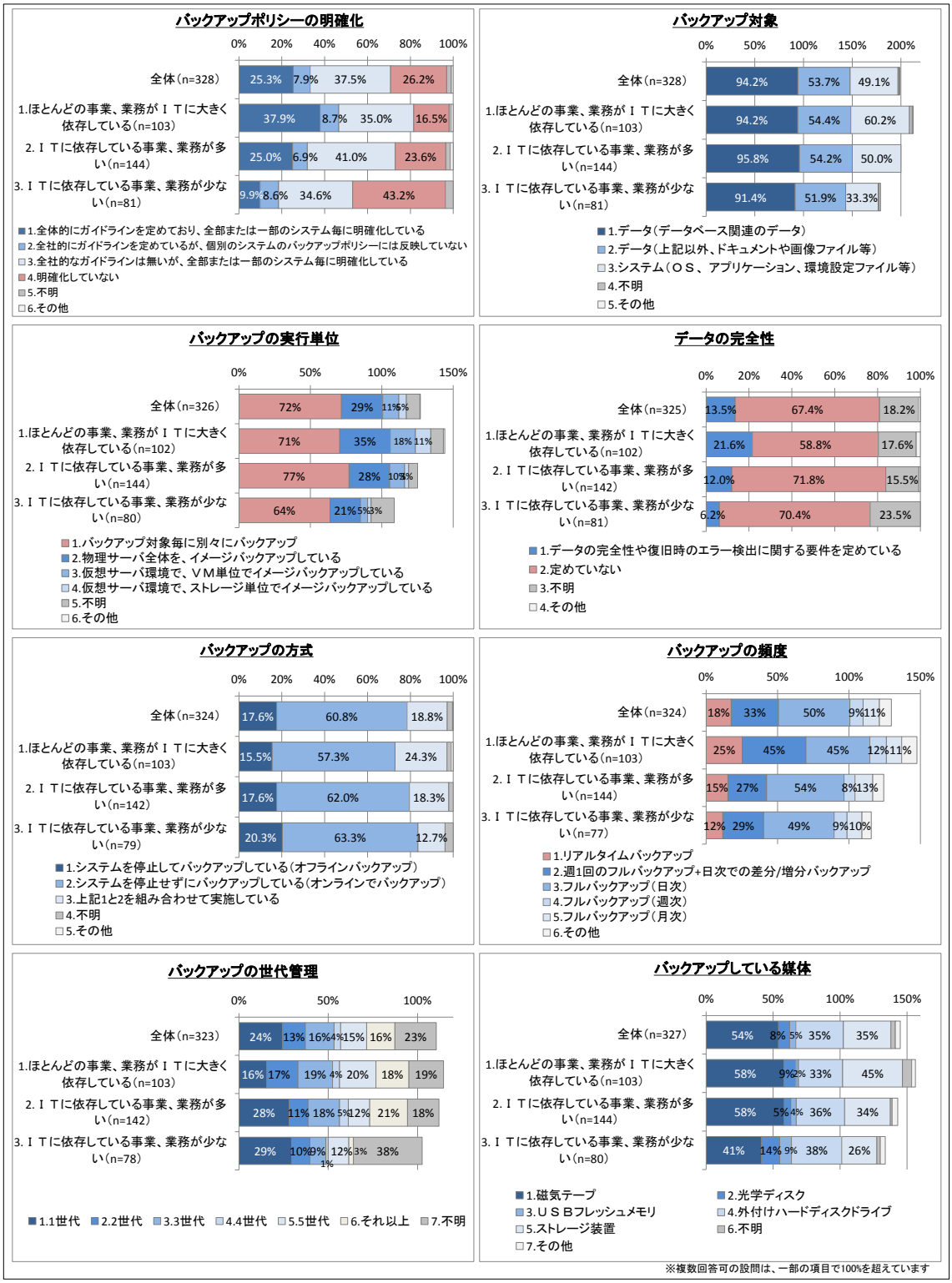


図 4-35 [事業の IT 依存度別] データの保管(バックアップ)実施状況(1/2)

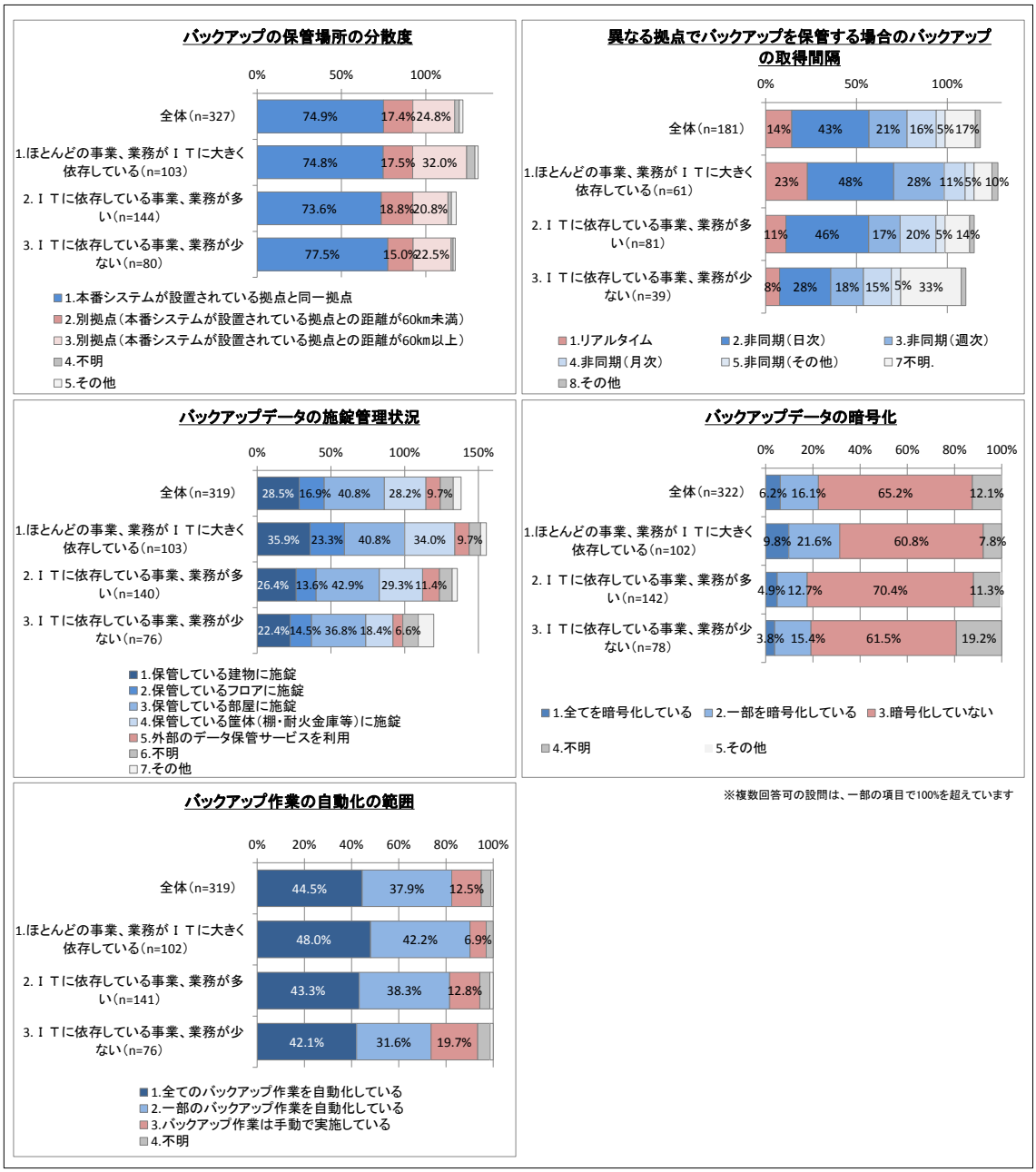


図 4-36 [事業の IT 依存度別] データの保管（バックアップ）実施状況(2/2)

⑥ 震災被害やその他の障害の経験とその後の対応

震災被害やその他の障害の経験とその後の対応について、調査を行った。

a. 震災等の経験とその後の対応

震災等で情報システムの利用を制限された経験をたずねたところ、東日本大震災で経験した企業が 29.3%と最も多い。一方、震災等により情報システムの利用の制限を経験しなかった企業は 62.8%となった(図 4-37)。

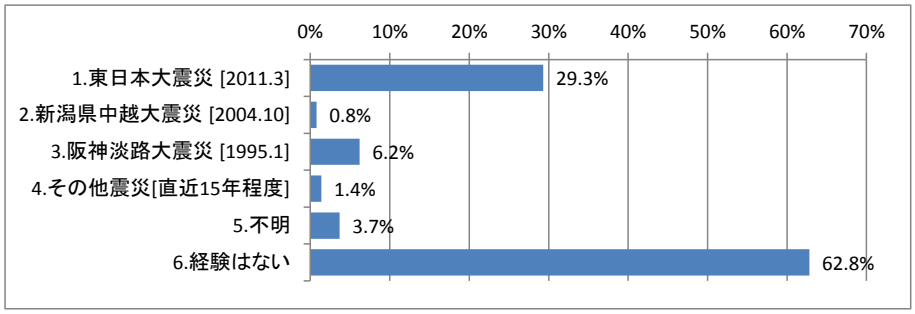


図 4-37 情報システムの利用を制限された経験のある震災(n=355)

東日本大震災等の震災後のデータの保管に対する認識の変化をたずねたところ、震災での情報システム利用制限の経験の有無により、異なる結果が見られた。全体では 36.2%の企業が「震災前の対策では不十分だと認識し、対策の検討を開始した」としているが、経験がある企業では 45.4%、経験が無い企業では 31.2%となっている(図 4-38)。自らの経験により必要性を実感した企業は、データが毀損・滅失することを、より切実な問題として捉えているのではないだろうか。

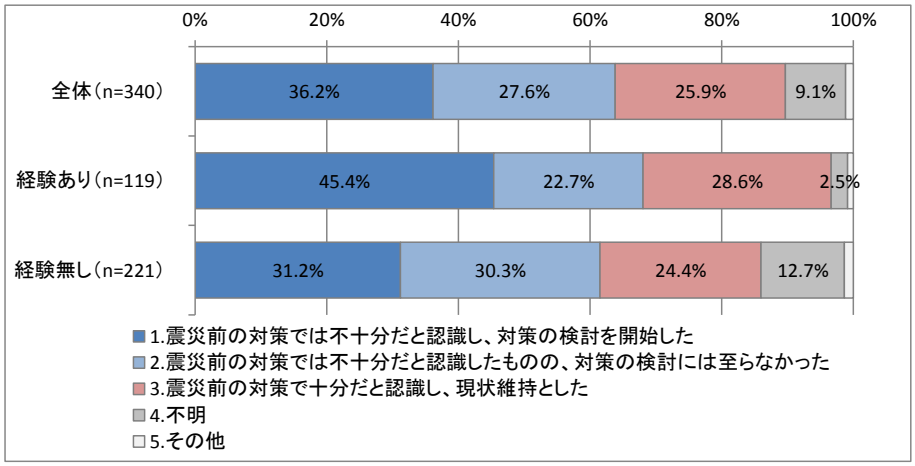


図 4-38 [震災による情報システムの利用制限の経験有無別] 東日本大震災等の震災後の、データの保管(バックアップ)に対する認識の変化

震災で経験したまたは今後懸念するデータの保管（バックアップ）に関する被害や問題は、「メインサイトのシステムのデータの滅失」が 72.6%と最も多く、次いで「バックアップ（データ）の滅失」が 56.5%、「バックアップの復元に時間がかかる」が 52.4%、「メインサイトのシステムのソフトウェアの滅失」が 45.2%となっている（図 4-39）。

また、震災後に検討を開始したデータの保管（バックアップ）に関する対策として、「バックアップの保管場所の分散度の見直し」が 43.5%と最も多く、対策の検討を行った企業の半数近くが挙げている。次いで、「バックアップ方式の見直し」が 39.5%、「バックアップポリシーの策定や見直し」と「バックアップ対象の見直し」が 33.1%となっている（図 4-40）。

文献調査では、今後取り組む対策に「災害発生時のシステム復旧手順」や「別拠点への重要データのバックアップ」が上位に挙げられていたり（図 2-9）、バックアップに関する意欲の変化に「遠隔バックアップの実施を開始したい」とする企業が 48.3%（図 2-13）あったりしたが、それらの傾向と同様の結果が得られている。

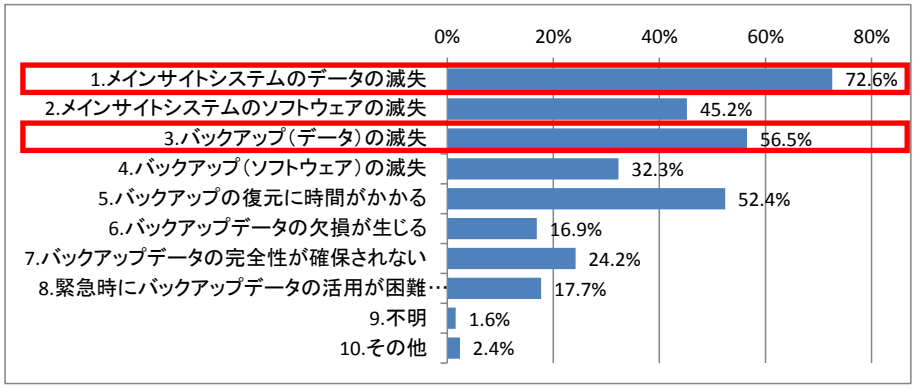


図 4-39 震災で経験したまたは今後懸念する、データの保管（バックアップ）に関する被害や問題（n=124）

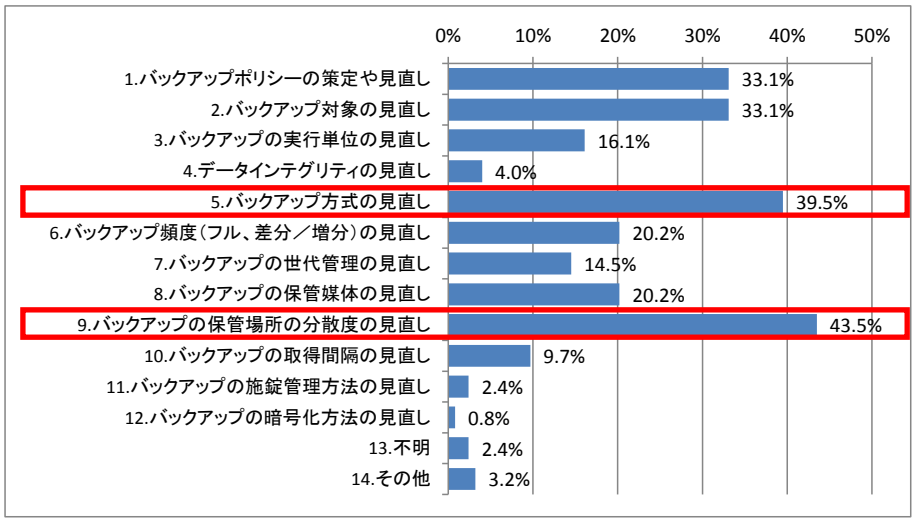


図 4-40 震災後に検討を開始したデータの保管（バックアップ）に関する対策（n=124）

b. 過去の復旧事例における問題点や有効な対策

過去にシステムの復旧において問題となった事項は、「復旧手順が未整備、手順が不明確」が21.4%と最も多く、次いで「必要なデータの消失」が20.4%、「電源を確保ができなかった」が19.5%、「通信を確保できなかった」が16.9%となっている（図 4-41）。

ここでも、2.1 における企業等の対策全般への意向と符合していることから、電源や通信等のインフラに関わる事項や、必要なデータの消失や復旧手順書の不備といった対策・運用に関わる事項は、企業において重点的に取り組むべき領域との認識が広まっていると理解することができる。

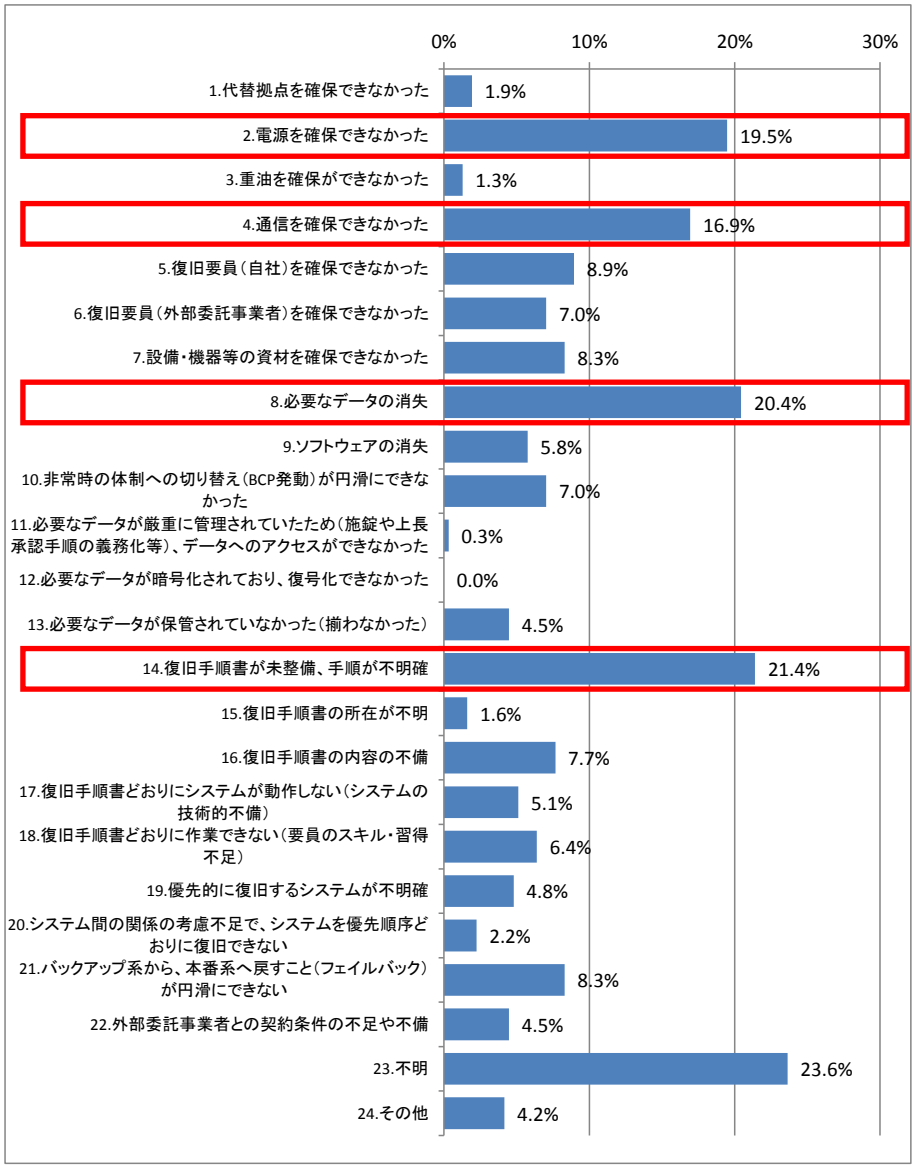


図 4-41 過去に、システムの復旧において、問題となった事項（n=313）

システム復旧に有効であった技術・サービスとして、「データセンタ」が 42.6%と最も多く挙げられており、次いで「仮想化技術」が 29.0%、「クラウドサービス」が 14.8%、「無線等を使った通信サービス」が 10.3%となっている（図 4-42）。データセンタはシステム設置サイトの耐障害性を向上させるだけでなく、バックアップサイトとしての役割を果たすことから、最も多く挙げられたのではないだろうか。仮想化技術やクラウドサービスには、概ね 1/3 程度の企業しか利用していない（図 4-12）にも関わらずこれだけの企業がシステム復旧への有効性を評価していることから、引き続きその効果の発揮が期待される。また、多くの企業が問題として挙げていたネットワークの冗長化については、無線等を使った通信サービスを有力な解決策の一つとして考えて良いのではないだろうか。

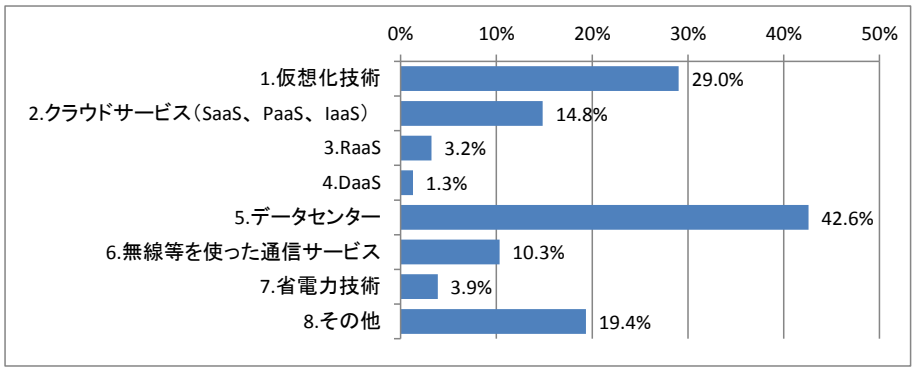


図 4-42 システム復旧に有効であった技術・サービス（n=155）

(2) 設問毎の回答集計結果

ここでは、アンケートの設問毎の回答の集計結果を示す。

① 企業プロフィール

設立年月日、資本金、本社所在地、本社所在地、拠点数、従業員数、業種、主な事業内容、事業の IT 依存度等の回答企業のプロフィールについてたずねた。

Q1.設立年月日

Q1.設立年月日について教えてください。

本質問項目では、回答企業の設立年月日をたずねた。回答を元に、事業継続期間を類型化した。設立後 20 年までの企業が 28.0%と最も多く、次いで「設立後 41 年～60 年」、「設立後 21 年～40 年」、「設立後 61 年～80 年」、「設立後 81 年以上」の順となっている(図 4-43)。

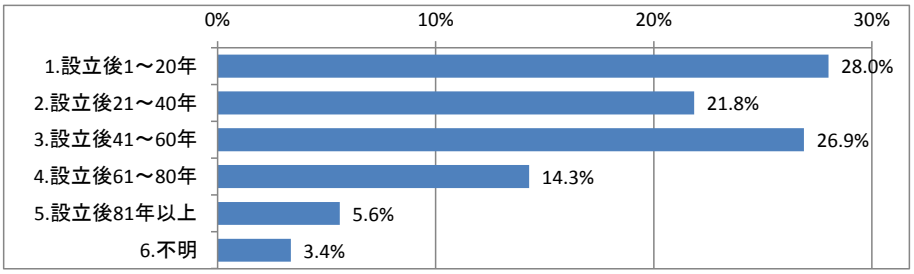


図 4-43 事業継続期間(n=357)

Q2.資本金

Q2.貴社の資本金を教えてください。(一つ選択)

資本金が「1 億円～3 億円未満」の企業が 45.3%最も多く、次いで「3 億円～5 億円未満」、「10 億円～50 億円未満」の順となっている(図 4-44)。

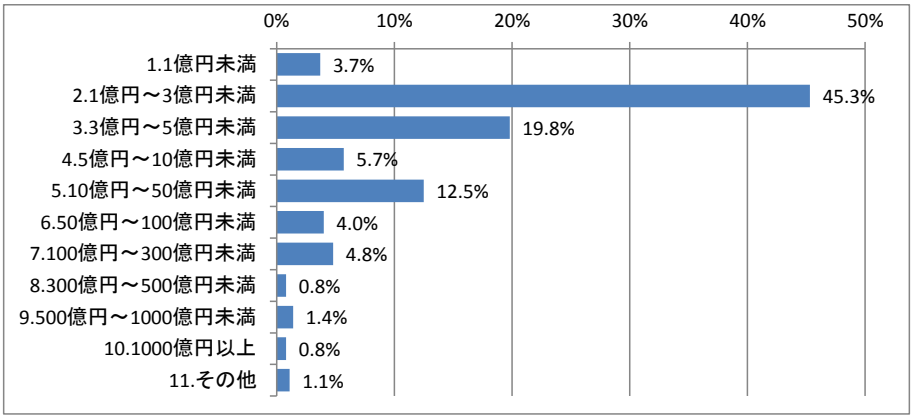
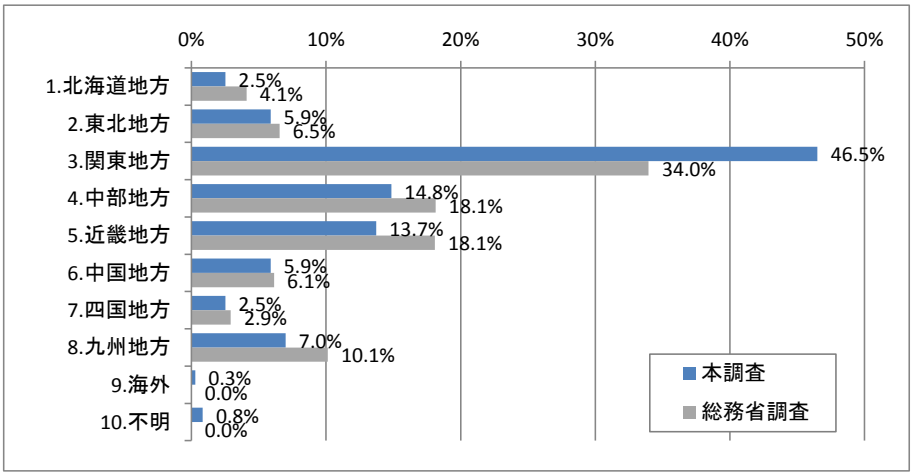


図 4-44 資本金(n=353)

Q3.本社所在地

Q3.貴社の本社所在地を教えてください。

本社所在地は、「関東地方」が 46.5%と最も多く、次いで「中部地方」、「近畿地方」、「九州地方」の順となり、「東北地方」、「四国地方」が同数、以下「北海道」、「海外」と続いている(図 4-45)。総務省統計局が平成 21 年に実施した調査における会社企業(本社・本店)の地域別分布状況と比較すると、本調査の企業分布は特に「関東地方」の割合が高い。総務省調査ではすべての規模の企業を対象としているのに対し、本調査では上場企業および非上場の資本金 1 億円以上を対象としていることから、比較的規模の大きい企業の分布割合が関東地方において高いことが要因の一つとして推察される。



出所:総務省統計局「平成 21 年経済センサス-基礎調査　企業等に関する集計第 16 表」(2011 年 6 月)より作成

図 4-45　本社所在地(n=357)

Q4.拠点数

Q4.貴社の拠点数を教えてください。(一つ選択)

拠点数は、「1 拠点～5 拠点」が 60.0%と最も多く、次いで「5 拠点～10 拠点未満」、「10 拠点～30 拠点未満」、「30 拠点～100 拠点未満」の順となっている(図 4-46)。

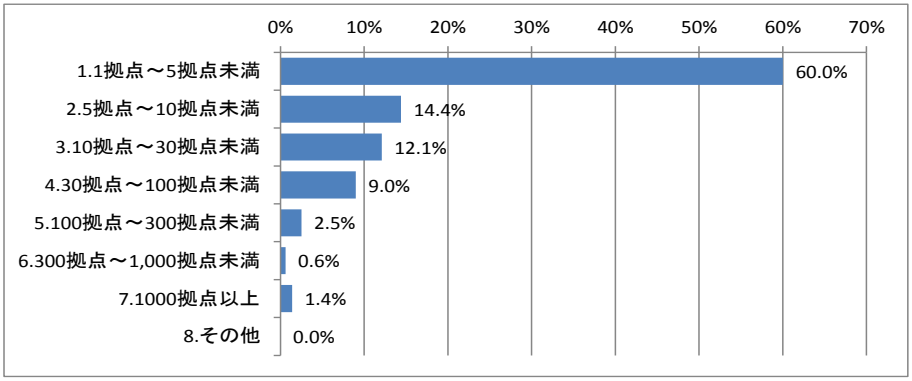


図 4-46　拠点数(n=355)

Q5.従業員数

Q5.貴社の従業員数について教えてください。(一つ選択)

従業員数は、「50 人～300 人未満」が 41.3%と最も多く、次いで「50 人未満」、「300 人～1,000 人未満」、「1,000 人～5,000 人未満」、「5,000 人～10,000 人未満」、「10,000 人以上」の順となっている(図 4-47)。

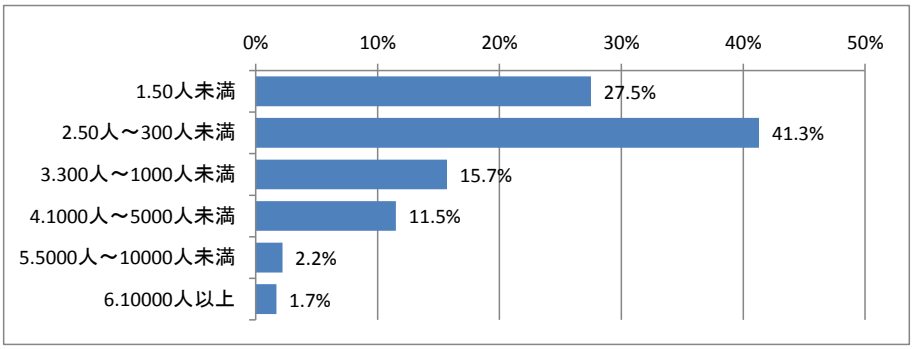


図 4-47 従業員数(n=356)

Q6.業種

Q6.貴社の業種を教えてください。(一つ選択)

回答企業の業種は、「製造業」が 31.7%と最も多く、次いで「サービス業」、「卸売・小売業、飲食店」、「運輸・通信業」、「不動産業」、「金融・保険業」、「建設業」、「電気・ガス・水道・熱供給業」の順となっている(図 4-48)。

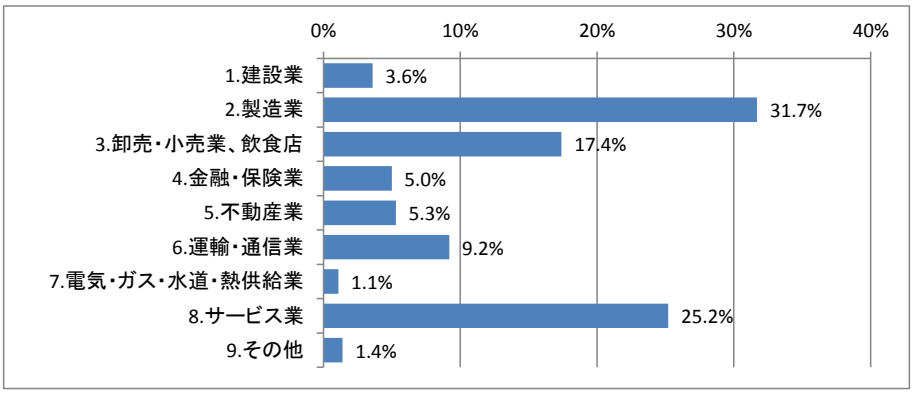


図 4-48 業種(n=357)

Q8.事業の IT 依存度

Q8.貴社の事業の IT 依存度について教えてください。(一つ選択)

「ほとんどの事業、業務が IT に大きく依存している」が 30.4%、「IT に依存している事業、業務が多い」が 43.4%、「IT に依存している事業、業務が少ない」が 26.2%となっている(図 4-49)。

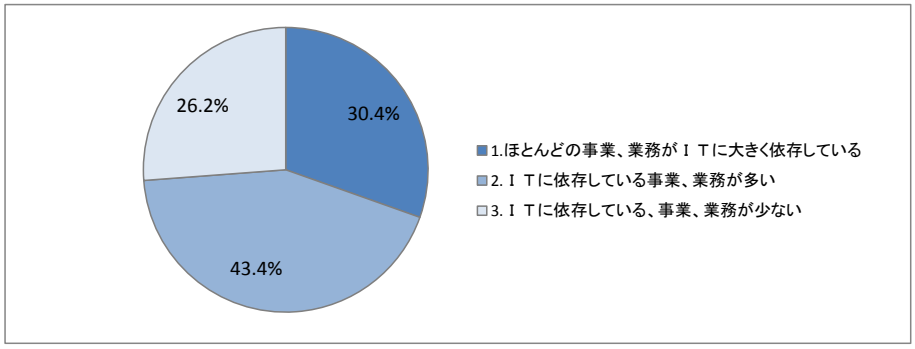


図 4-49 事業の IT 依存度(n=355)

② IT サービス継続に関する取り組み状況

IT サービス継続に関する取り組み状況についてたずねた。

Q9.事業継続計画

Q9.貴社の事業継続計画の策定状況について教えてください。(一つ選択)

事業継続計画を「策定済み」としている企業は 40.1%、「未策定(検討中)」としている企業は 33.1%、「未策定(予定なし)」としている企業が 18.6%となっている(図 4-50)。「策定済み」および「未策定(検討中)」と回答した 73.2%の企業が事業継続に対する関心を持ち、具体的な取り組みを進めているまたは進めようとしている。

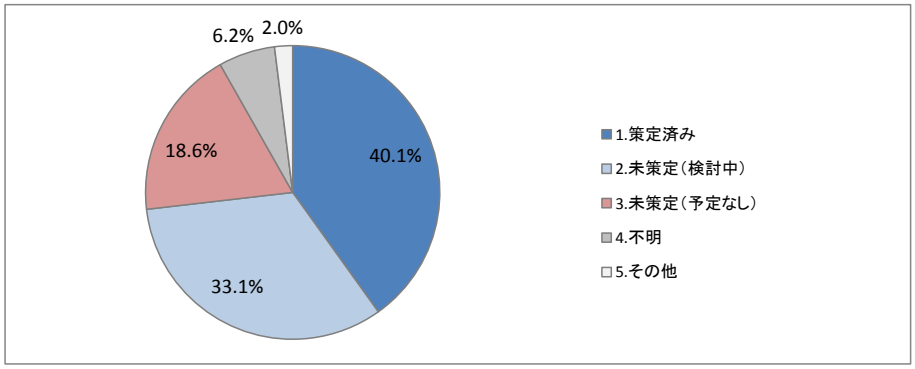


図 4-50 事業継続計画(n=354)

Q10.情報システム部門における事業継続計画(IT サービス継続計画、IT-BCP)

Q10.貴社の情報システム部門における、事業継続計画(IT サービス継続計画、IT-BCP)の策定状況について教えてください。(一つ選択)

情報システム部門における事業継続計画(IT サービス継続計画、IT-BCP)を「策定済み」としている企業は 24.8%、「未策定(検討中)」としている企業は 40.9%、「未策定(予定なし)」としている企業が 27.4%となっている(図 4-51)。BCP の策定状況と比較すると、具体的な取り組みを進めている企業は少ないものの、2/3(65.7%:「策定済み」および「未策定(検討中)」の合計)の企業は、IT-BCP 対して前向きに取り組んでいる。

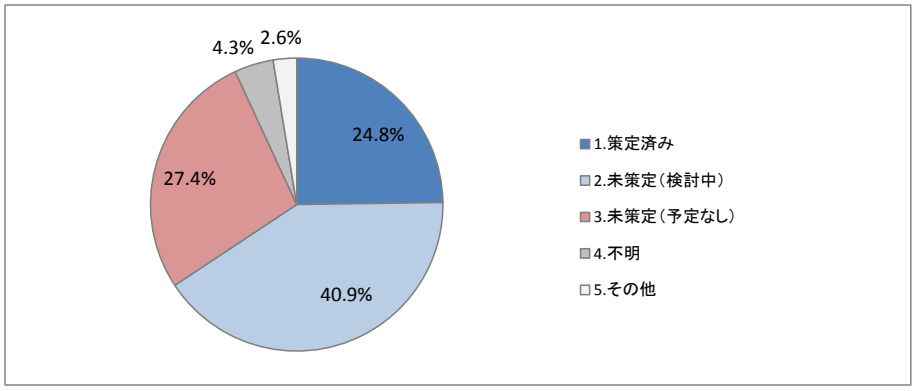


図 4-51 情報システム部門における、事業継続計画(IT-BCP)(n=347)

Q11.IT サービス継続に関する取り組み状況

Q11. IT サービス継続に関して、貴社では以下の取り組みを組織として実施していますか。

1. 事業継続のために重要となる業務の維持に必要な IT サービスを特定している
2. ビジネスインパクト分析(業務影響度分析)を実施している
3. 重要業務の目標復旧時間等を考慮して、IT サービスの目標復旧時間等を定めている
4. IT サービスの中断、停止に備えた事前対策(代替システムやデータ保護、耐震強化等)を定めた対策実施計画を策定している
5. IT サービスの中断、停止に備えた、システム担当者等の教育訓練内容を定めた教育訓練計画を策定している
6. IT サービスが中断、停止した場合に、復旧するための対応体制、手順等を定めた事後対策計画や緊急時対応計画を策定している
7. IT サービス継続の取り組みの継続的な維持改善を行うための管理方法を定めた維持改善計画を策定している

情報システム部門における事業継続計画を「策定済み」または「未検討(検討中)」と回答した企業に、IT サービス継続に関する取り組み状況をたずねた。事業継続のために必要な IT サービスを特定している企業は 52.2%となった。一方、「ビジネスインパクト分析(業務影響度分析・BIA)を実施してい

る」が 25.0%、「重要業務の目標復旧時間等を考慮して、IT サービスの目標復旧時間等を定めている」が 28.1%、「IT サービスの中断、停止に備えた事前対策（代替システムやデータ保護、耐震強化等）を定めた対策実施計画を策定している」が 39.5%、「IT サービスの中断、停止に備えた、システム担当者等の教育訓練内容を定めた教育訓練計画を策定している」が 19.7%、「IT サービスが中断、停止した場合に、復旧するための対応体制、手順等を定めた事後対策計画や緊急時対応計画を策定している」が 29.8%、「IT サービス継続の取り組みの継続的な維持改善を行うための管理方法を定めた維持改善計画を策定している」が 17.1%となっている（図 4-52）。

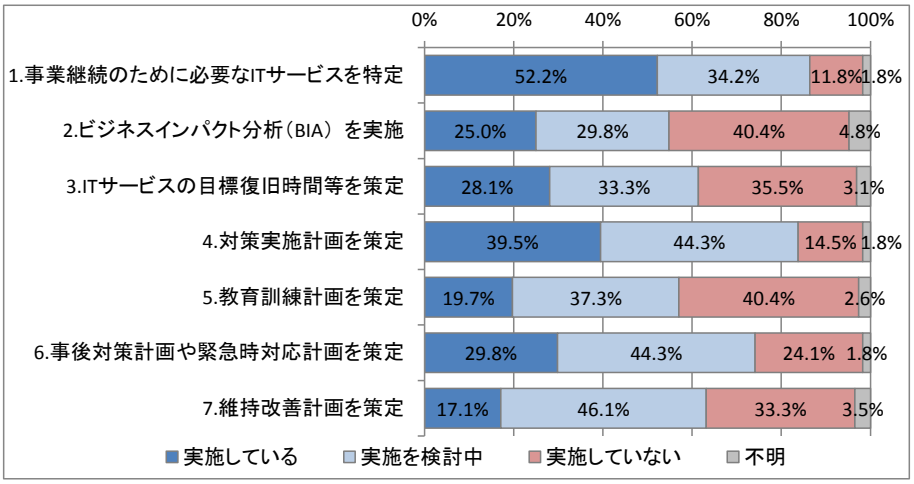


図 4-52 IT サービス継続に関する取り組み状況（n=227）

Q12.IT サービス継続計画策定時に想定するリスク

Q12.IT サービス継続計画策定時の想定するリスクを教えてください。（複数選択可）

IT サービス継続計画策定時の想定リスクとして、7 割を超える企業が「自然災害（直下型地震による局所被害）」と「自然災害（大規模地震による広域被害）」を挙げている。次いで、「停電」が 64.4%、「ハードウェアの故障」が 63.6%、「通信回線の故障」が 56.9%、「建物や施設の破壊・損失」が 51.6%となっている（図 4-53）。東日本大震災ではインフラ面のリスクが大きくクローズアップされた。震災から 1 年以上経過したとはいえ、引き続きインフラ面のリスクに着目している企業が多いことが推察される。

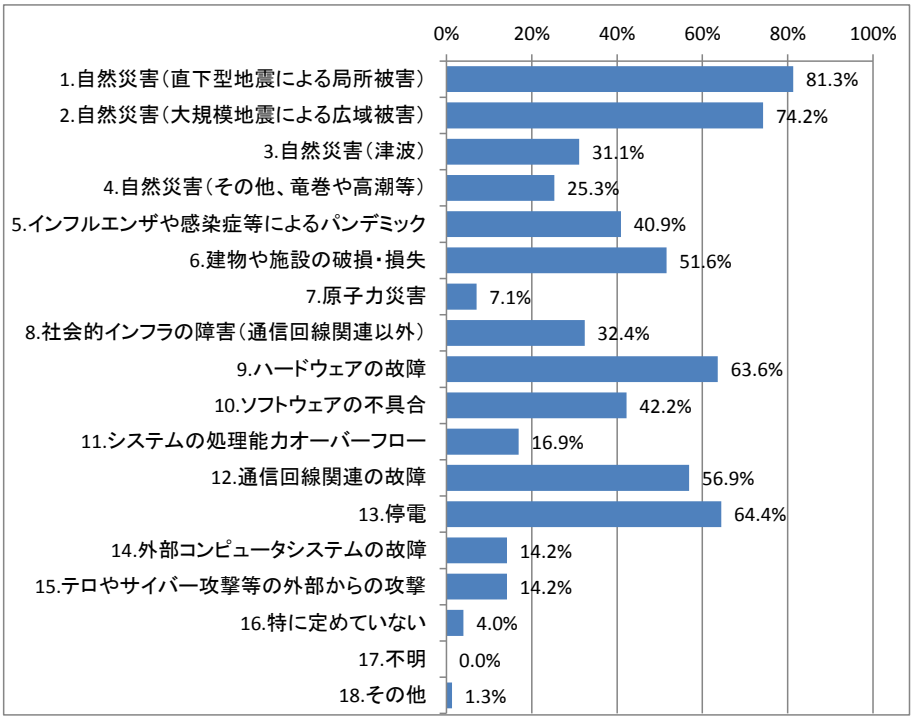


図 4-53 IT サービス継続計画策定時に想定するリスク（n=225）

Q13.重点的に取り組んでいる領域

Q13.IT サービス継続について、重点的に取り組んでいる領域について教えてください。（複数選択可）

IT サービス継続において、重点的に取り組んでいる領域として「冗長化された電源供給やネットワーク」、「データの遠隔地保管」、「情報処理設備や機器の冗長化」を半数程度の企業が挙げている。それに続いて、「耐震構造の建物やバックアップサイト」、「システム運用の仕組みや体制」、「OS 等やデータの冗長化」と並んでいるが、どの領域も少なくない企業が重点的に取り組んでいる（図 4-54）。

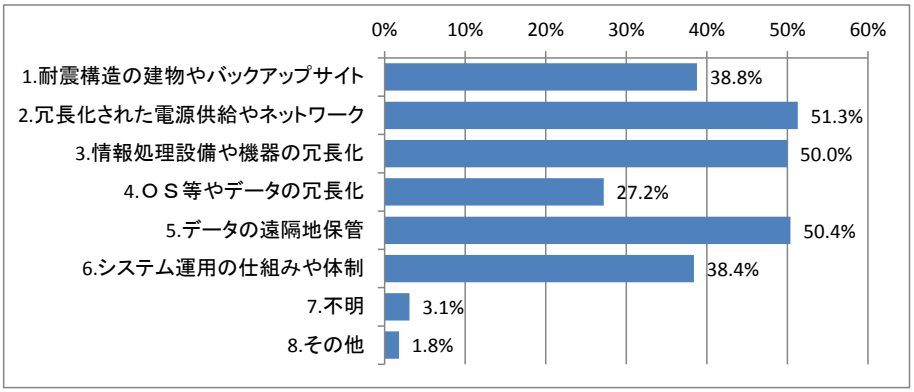


図 4-54 重点的に取り組んでいる領域（n=224）

Q14.リカバリ要件定義やバックアップポリシー策定の際に参照した規格やガイドライン等

Q14.リカバリ要件定義やバックアップポリシー策定の際に参照した規格やガイドライン等について教えてください。(複数選択可)

IT サービス継続計画を策定する上での重要事項として、リカバリ要件定義やバックアップポリシーが挙げられるが、それらを策定する際に参照した規格やガイドラインをたずねた。「IT サービス継続ガイドライン(経産省)」が 44.3%と最も多く、次いで「事業継続ガイドライン(内閣府)」が 30.2%、「ISO/IEC27001,27002/JISQ27001,27002」が 17.4%と続いている(図 4-55)。「その他」の内訳としては、主に親会社やグループ会社のガイドラインが挙げられている。最も多く参照されているのが経産省や総務省が発行しているガイドラインであることから、IT サービス継続における国の取り組みに大きな期待が寄せられていると考えることができる。

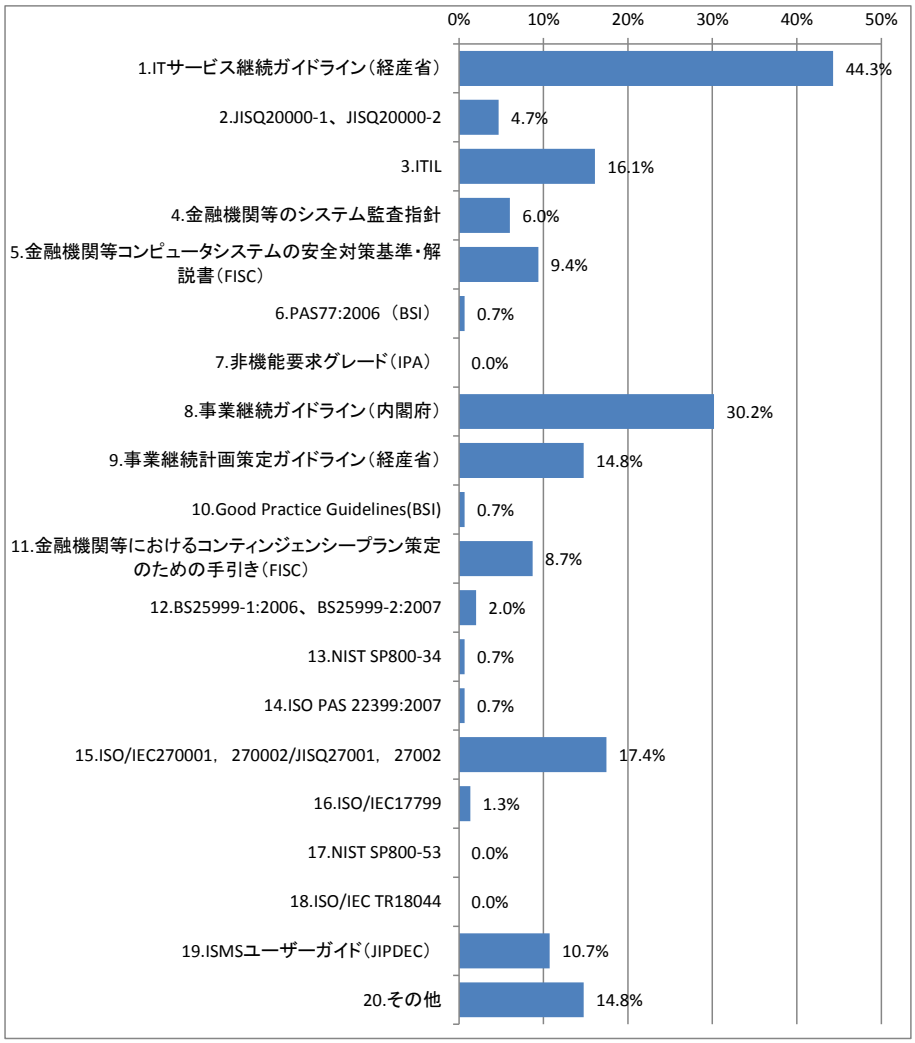


図 4-55 リカバリ要件定義やバックアップポリシー策定の際に参照した規格やガイドライン等(n=149)

③ コンピュータシステムと新しい技術の採用状況

コンピュータシステムを運用している業務およびシステム、仮想化技術やクラウドサービスといった新しい技術の採用状況をたずねた。

Q15.コンピュータシステムを運用している業務

Q15.コンピュータシステムを運用している業務（複数選択可）

96.1%の企業が「財務・会計」を、82.6%が「人事・給与」を挙げており、8割以上の企業が両業務においてコンピュータシステムを運用していると回答している。次いで、「販売」、「生産・サービス提供」、「調達」、「開発・設計」、「物流」、「カスタマーサポート」となっている（図 4-56）。

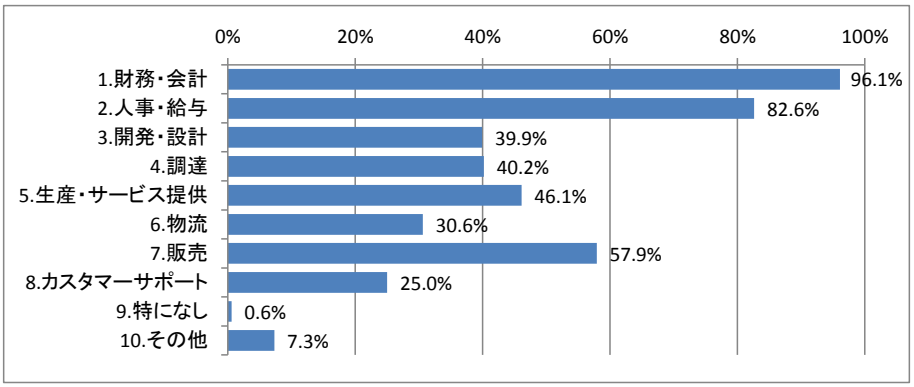


図 4-56 コンピュータシステムを運用している業務（n=356）

Q16.Q15 の業務で運用しているシステムのうち、事業継続において最も影響の大きいシステム

Q16.Q15 の業務で運用しているシステムのうち、事業継続において最も影響の大きいシステムについて教えてください。（複数選択可）

65.3%が「財務・会計管理システム」を、43.4%が「販売管理システム」を、29.1%が「メール・グループウェア」を挙げている（図 4-57）。

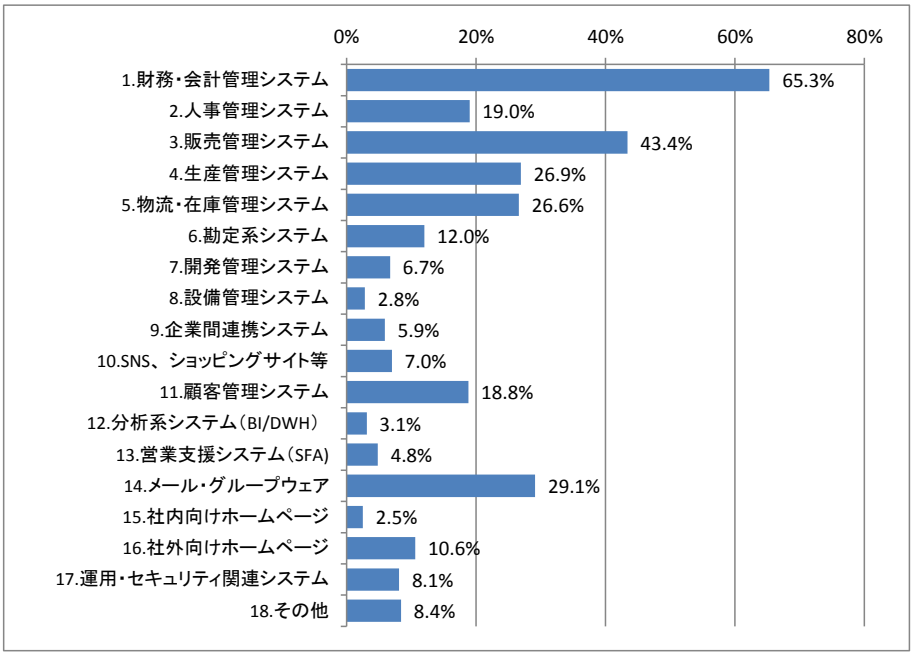


図 4-57　Q16.Q15 の業務で運用しているシステムのうち、事業継続において最も影響の大きいシステム（n=357）

Q17.データの保管（バックアップ）対象となっているシステム

Q17.Q16 で選択したシステムのうち、データの保管（バックアップ）対象となっているシステムを教えてください。（複数選択可）

65.0%の企業が「財務・会計管理システム」を、45.3%が「販売管理システム」を、28.9%が「生産管理システム」を、27.1%が「物流・在庫管理システム」を、29.1%が「メール・グループウェア」を挙げている（図 4-58）。Q16 の傾向と比較すると、上位 2 件のシステムは同様の順番であるものの、「生産管理システム」や「物流・在庫管理システム」が上位となり、「メール・グループウェア」が下位になっている。

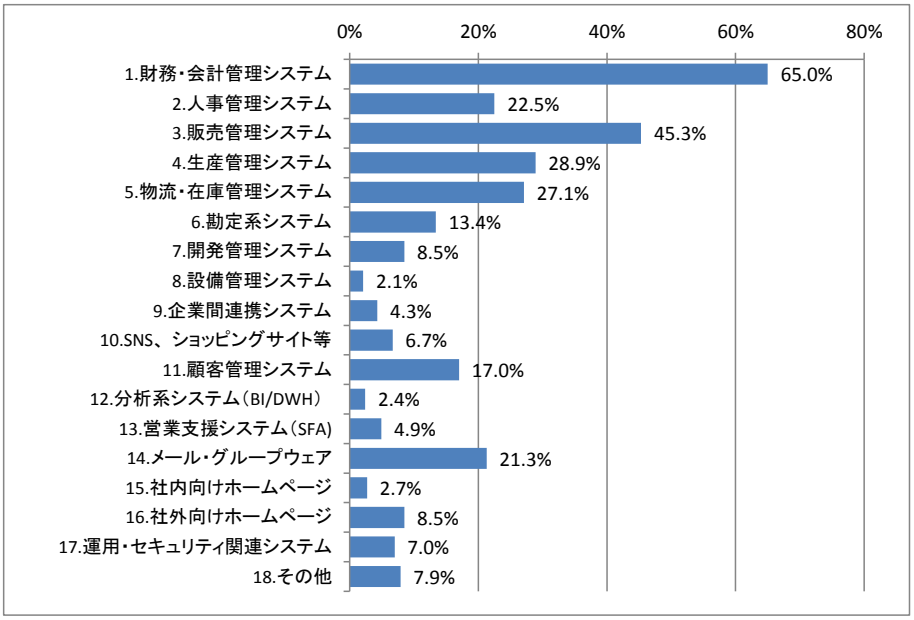


図 4-58　データの保管（バックアップ）対象となっているシステム（n=329）

Q18.仮想化技術の利用状況

Q18.Q16 でお伺いした事業継続において最も影響の大きいシステムについてお伺いします。仮想化技術の利用状況について教えてください。（一つ選択）

仮想化技術を「利用している」と「利用していない（検討中）」を合わせて 48.7%となっており、半数近くの企業が仮想化技術の採用に前向きな姿勢を見せている。一方、45.1%の企業は「利用していない（予定無し）」となっている。事業継続において最も影響の大きいシステムにおいては、半数近くの企業は仮想化技術の利用に消極的である（図 4-59）。

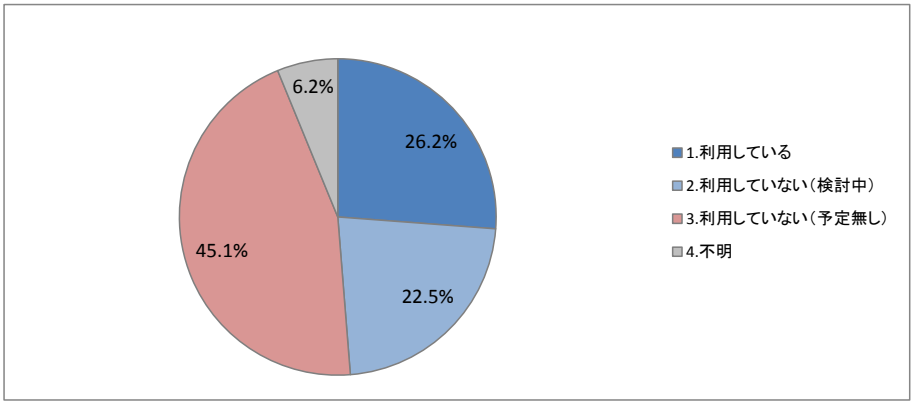


図 4-59　仮想化技術の利用状況（n=355）

Q19.仮想化技術の導入対象

Q19.Q18 で仮想化技術を「1. 利用している」、「2. 利用していない（検討中）」の方にお伺いします。仮想化技術の導入対象について教えてください。（複数選択可）

仮想化技術を利用している企業のうち、94.6%の企業が「サーバ」を対象に導入している。次いで、「ストレージ」が 34.3%、「クライアント端末」が 16.9%、「ネットワーク」が 13.9%と続いている（図 4-60）。仮想化の導入対象としてほとんどの企業が「サーバ」を挙げていることから、「仮想化」というとサーバが一般的で、それ以外の分野はこれからの普及分野とも考えられる。

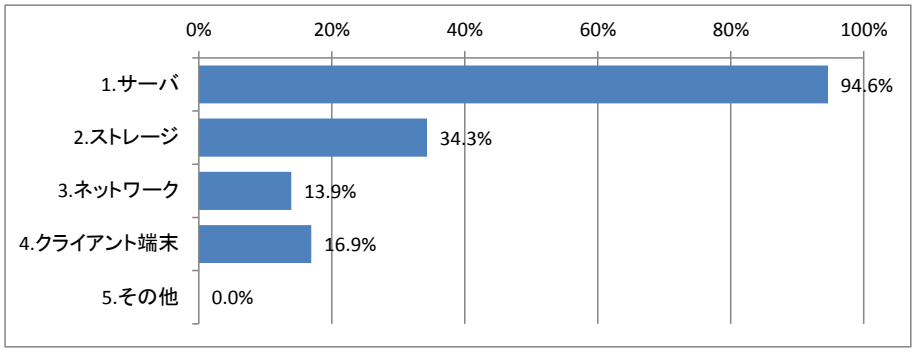


図 4-60 仮想化技術の導入対象（n=166）

Q20.クラウドサービスの利用状況

Q20.Q16 でお伺いした事業継続において最も影響の大きいシステムについてお伺いします。クラウドサービスの利用状況について教えてください。（一つ選択）

クラウドサービスを「利用している」と「利用していない（検討中）」を合わせて 40.2%となっている。一方、55.2%の企業は「利用していない（予定無し）」となっている（図 4-61）。事業継続において最も影響の大きいシステムにおいては、仮想化技術の導入状況と比較すると相対的に普及が進んでいないと考えることができる。

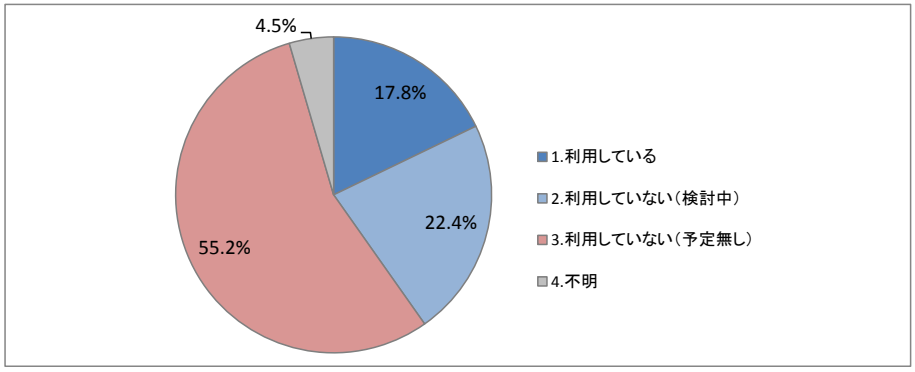


図 4-61 クラウドサービスの利用状況（n=353）

Q21.クラウドサービスの導入目的

Q21.クラウドサービスの導入目的について教えてください。(複数選択可)

クラウドサービスの導入目的として「運用・保守費用の低減(機器の削減、料金の削減)」が 61.7%と最も多く挙げられており、次いで「災害への対策」が 56.7%、「導入費用の低減」が 48.2%、「運用要員の削減・負担軽減」が 41.1%となっている(図 4-62)。

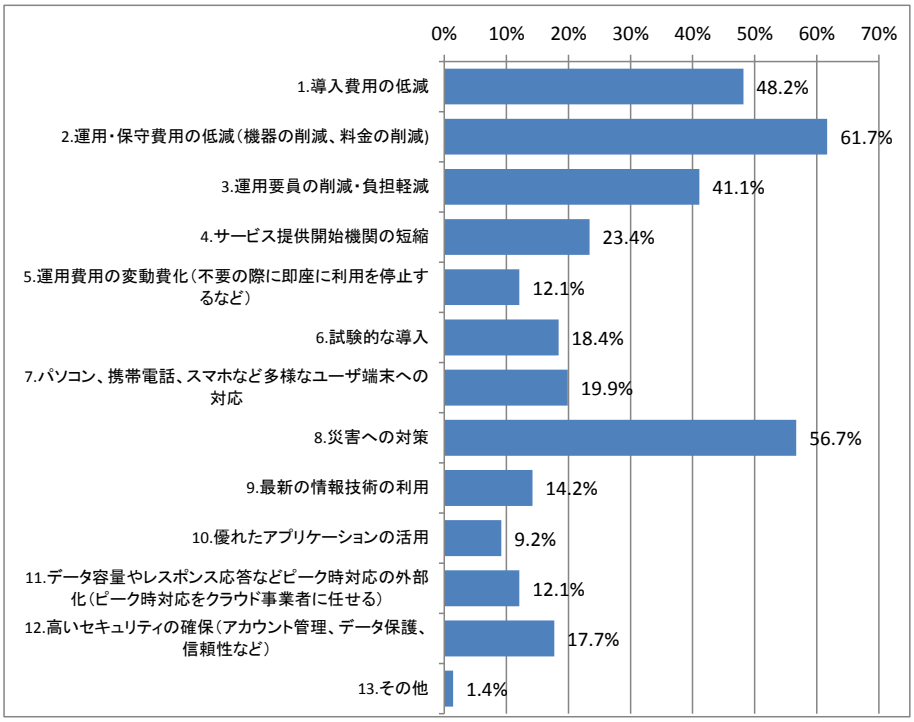


図 4-62 クラウドサービスの導入目的(n=141)

Q22.利用中のクラウドサービスの種類

Q22.利用中または利用検討中のクラウドサービスの種類を教えてください。(複数選択可)

62.1%の企業がクラウドサービスとして「SaaS」を利用している。次いで、「PaaS」が 25.9%、「IaaS」が 12.1%、「RaaS」が 10.3%、「DaaS」が 7.8%と続いている(図 4-63)。

なお、本アンケート調査では、各サービスの種類を次のように定義している。

- SaaS:ソフトウェアをサービスとして提供
- PaaS:アプリケーションを稼働させるための基盤(プラットフォーム)をサービスとして提供
- IaaS:サーバ、CPU、ストレージなどのインフラをサービスとして提供
- RaaS:システム回復を目的としたクラウド上のシステムやデータのバックアップ・リカバリサービス
- DaaS:クラウドを利用したデスクトップ環境の仮想化

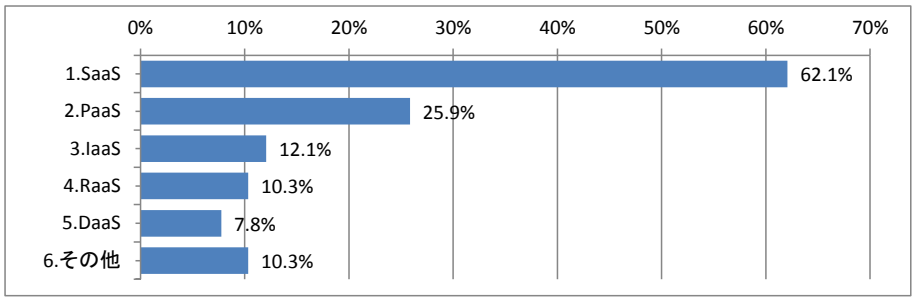


図 4-63 利用中のクラウドサービスの種類(n=116)

④ システム構成

事業継続に最も影響の大きいシステムにおける、コンピュータシステムの冗長化の状況と障害発生時の復旧作業の手順についてたずねた。

Q23.システム(サーバ)の冗長化の状況

Q23.システム(サーバ)の冗長化の状況について教えてください。(複数選択可)

「冗長化していない」企業が42.1%と最も多く、次いで「同一サイト(メインサイト)内に待機系システムを設置」が 37.3%、「バックアップサイト(遠隔地)に待機系システムを設置」が 15.5%となっている(図4-64)。

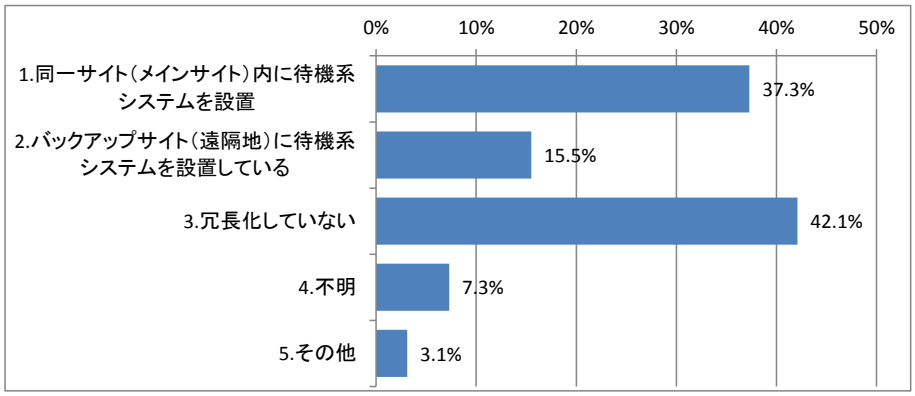


図 4-64 システム(サーバ)の冗長化の状況(n=354)

Q24.待機系システムの状態

Q24.待機系システムの状態について教えてください。(一つずつ選択)

同一サイトにおける待機系システムの状態は、「コールドスタンバイ」が 25.7%、「ウォームスタンバイ」が 26.5%、「ホットスタンバイ」が 38.1%となっている(図 4-65 上段)。バックアップサイトにおける待機系システムの状態は、「コールドスタンバイ」が 25.6%、「ウォームスタンバイ」が 35.9%、「ホットスタンバイ」が 17.9%となっている(図 4-65 下段)。

なお、本設問においては待機状態を次のように定義してたずねている。

・コールドスタンバイ:電源投入や設定等がなされていない状態で待機

・ウォームスタンバイ:障害発生時に一定の作業で切り替えられる状態で待機

・ホットスタンバイ:本番システムと同様の構成で起動し待機

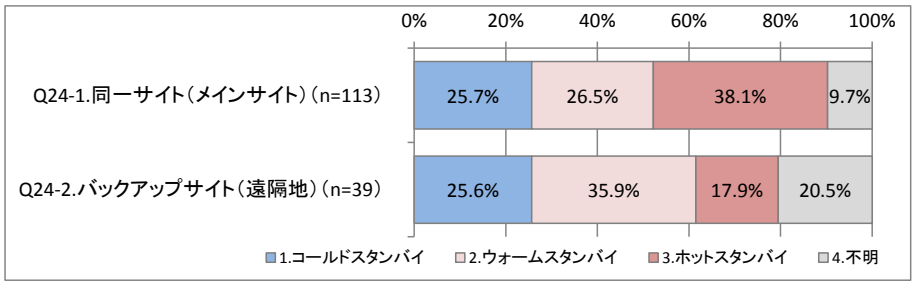


図 4-65 待機系システムの状態

Q25.障害発生時の復旧作業の自動化の状況

Q25.障害発生時の復旧作業の自動化の状況について教えてください。(一つずつ選択)

同一サイトにおける復旧作業の自動化の状況は、「一部自動化」と「全て自動化」が 45.0%と両者同様の割合となっている(図 4-66 上段)。バックアップサイトにおける復旧作業の自動化の状況は、「一部自動化」が 20.5%、「全て自動化」が 53.8%となっている(図 4-66 下段)。バックアップサイト(遠隔地)での復旧作業は、手作業で実施する割合が高い。

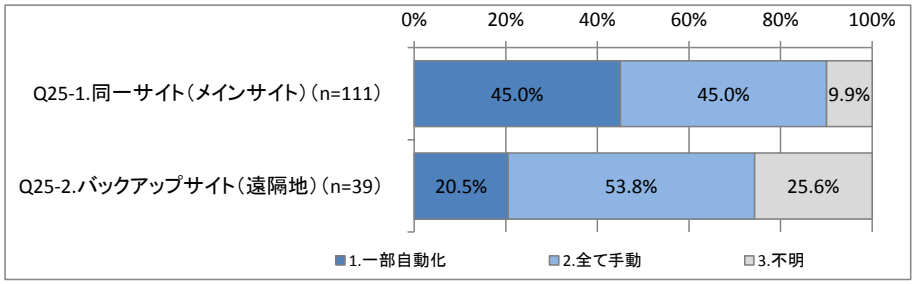


図 4-66 障害発生時の復旧作業の自動化の状況

⑤ リカバリ要件定義の有無と内容

事業継続に最も影響の大きいシステムにおける、リカバリ要件定義の有無と内容をたずねた。

Q26.目標復旧時間(RTO)の設定

Q26. 目標復旧時間(RTO)設定の有無と内容について教えてください。(それぞれ一つ選択)

目標復旧時間(RTO)は、21.1%が「策定済み」、28.0%が「未策定(検討中)」と回答し、半数の企業が復旧目標の定量化に取り組む姿勢が見られる(図 4-67)。

設定している時間について、目標復旧時間(RTO)を「策定済み」と「未策定(検討中)」と回答した企業にたずねたところ、「1 時間～6 時間未満」が 28.0%と最も多く、次いで「6 時間～24 時間」が 18.5%、「1 日～1 週間」が 15.5%となっている(図 4-68)。

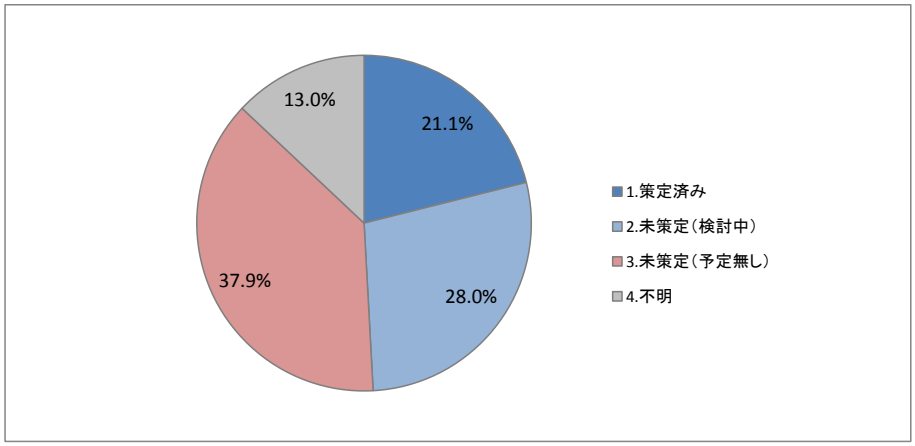


図 4-67 目標復旧時間(RTO)設定の有無(n=346)

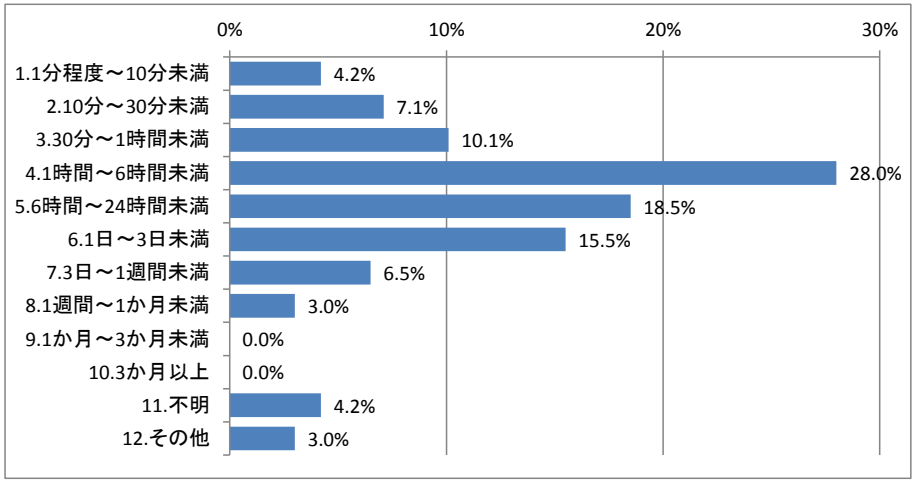


図 4-68 目標復旧時間(RTO)の設定条件(n=168)

Q27.目標復旧レベル(RLO)の設定

Q27. 目標復旧レベル(RLO)設定の有無と内容について教えてください。(それぞれ一つ選択)

目標復旧レベル(RLO)は、20.2%が「策定済み」、29.0%が「未策定(検討中)」と回答している(図4-69)。

設定している水準について、目標復旧レベル(RLO)を「策定済み」と「未策定(検討中)」と回答した企業にたずねたところ、「障害・被災前と同等の業務を実施できる水準」が 42.1%と最も多く、次いで「障害・被災前より低い性能(パフォーマンス)水準」が 27.4%、「障害・被災前より業務・昨日を制限した水準」が 14.0%、「障害・被災前より利用できる場所や端末を制限した水準」が 9.8%となっている(図4-70)。

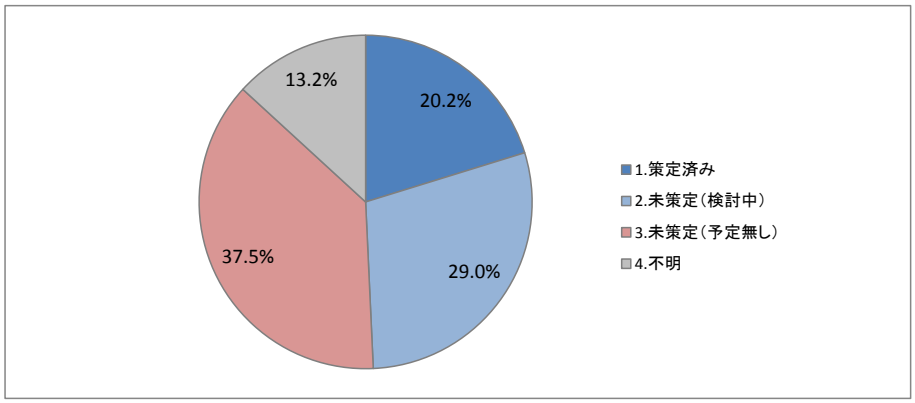


図 4-69 目標復旧レベル(RLO)設定の有無(n=341)

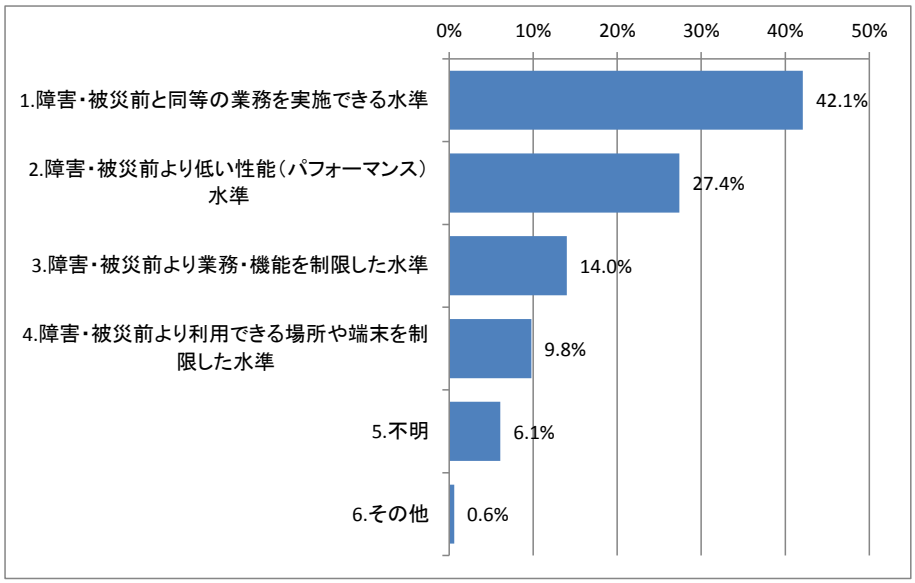


図 4-70 目標復旧レベル(RLO)の設定条件(n=164)

Q28.目標復旧時点（RPO）の設定

Q28. 目標復旧時点（RPO）設定の有無と内容について教えてください。（それぞれ一つ選択）

目標復旧時点（RPO）は、18.8%が「策定済み」、28.8%が「未策定（検討中）」と回答している（図 4-71）。

設定している水準について、目標復旧時点（RPO）を「策定済み」と「未策定（検討中）」と回答した企業にたずねたところ、「障害・被災発生前の前日まで復旧」が 48.1%と最も多く、次いで「障害・被災発生の直前まで復旧」が 35.6%、「障害・被災発生の 1 週間前まで復旧」が 6.9%、「障害・被災発生の 1 か月前まで復旧」が 2.5%となっている（図 4-72）。

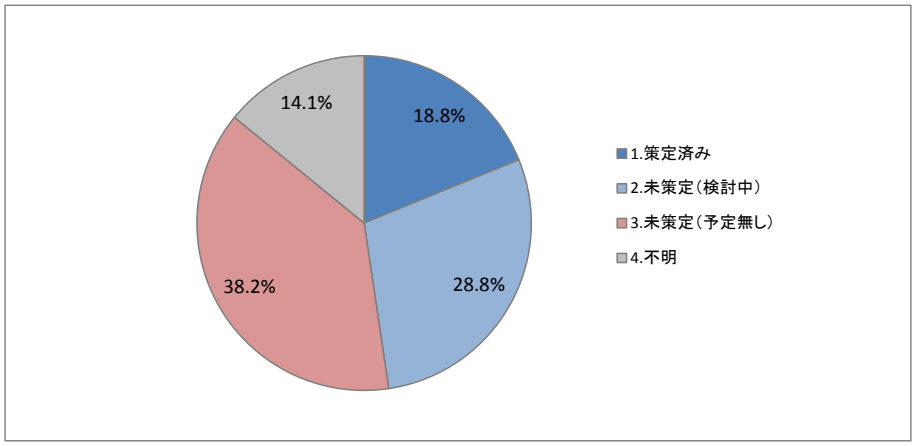


図 4-71 目標復旧時点（RPO）設定の有無（n=340）

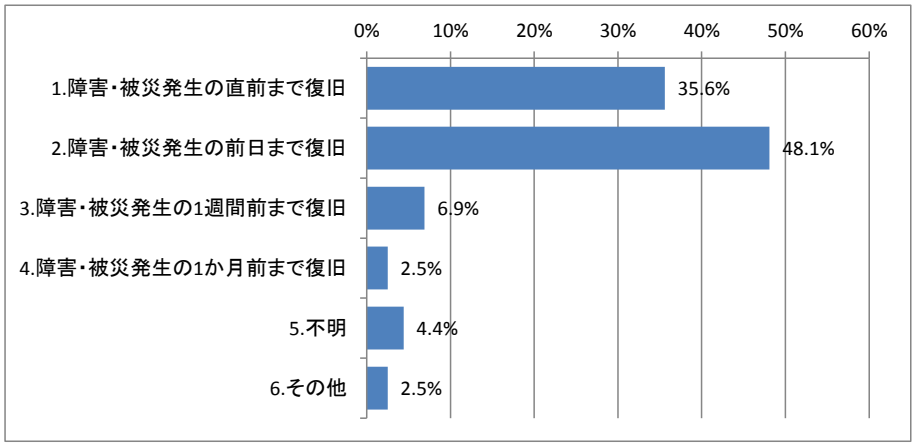


図 4-72 目標復旧時点（RPO）の設定の条件（n=160）

⑥ データの保管（バックアップ）状況

事業継続に最も影響の大きいシステムにおける、データの保管（バックアップ）対策について、バックアップポリシーの策定状況のほか、バックアップの対象や頻度など、具体的な対策状況についてたずねた。

Q29.データの保管（バックアップ）の実施状況

Q29. データの保管（バックアップ）の実施状況について教えてください。（一つ選択）

92.7%の企業が事業継続に最も影響の大きいシステムのデータ保管（バックアップ）を実施している（図 4-73）。

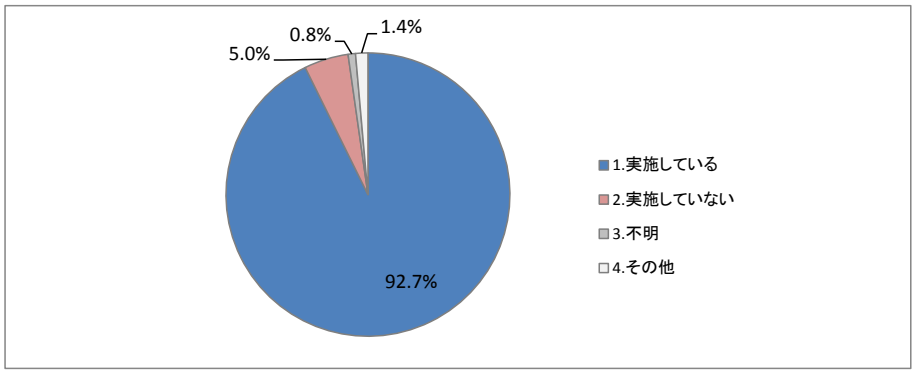


図 4-73 データの保管（バックアップ）の実施状況（n=357）

Q30.バックアップポリシーの明確化

Q30. バックアップポリシーの明確化について教えてください。（一つ選択）

「全社的にガイドラインを定めており、全部または一部のシステム毎に明確化している」および「全社的にガイドラインを定めているが、個別のシステムのバックアップポリシーには反映していない」を合わせて 33.1%となっている。「全社的なガイドラインは無いが、全部または一部のシステム毎に明確化している」を合わせると 71.0%の企業が何らかの形でバックアップポリシーを明確化している（図 4-74）。

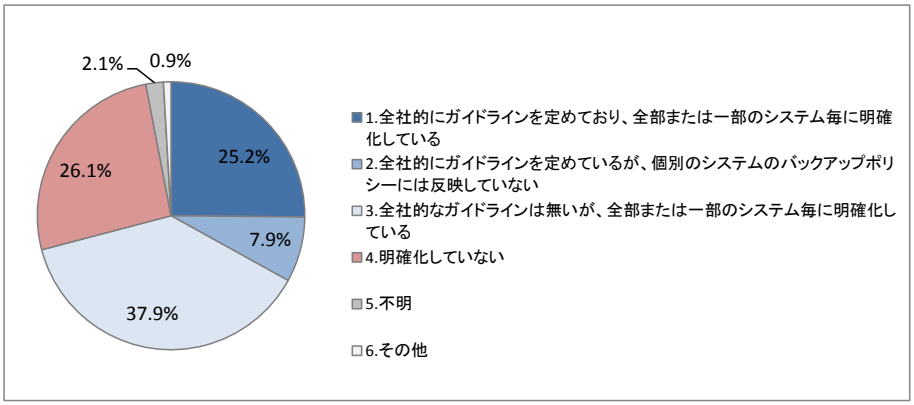


図 4-74 バックアップポリシーの明確化(n=330)

Q31.バックアップ対象

Q31. バックアップ対象について教えてください。(複数選択可)

94.2%の企業が「データ(データベース関連のデータ)」をバックアップ対象としている。53.6%が「データ(ドキュメントや画像ファイル等)を、48.8%が「システム(OS、アプリケーション、環境設定ファイル等)」を対象としている(図 4-75)。

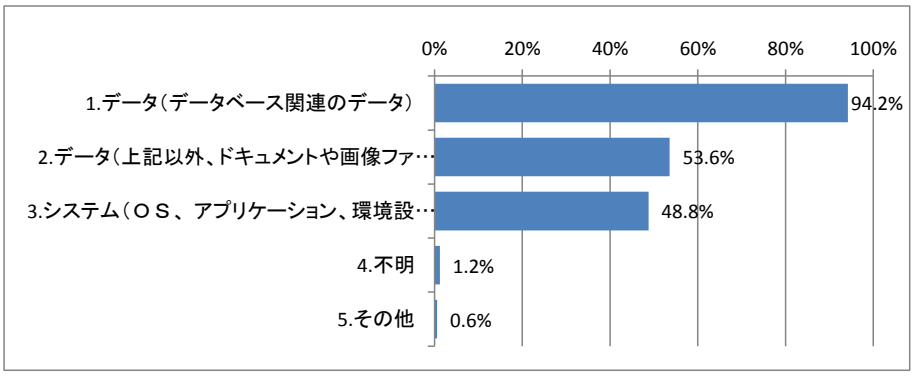


図 4-75 バックアップ対象(n=330)

Q32.バックアップの実行単位

Q32. バックアップの実行単位について教えてください。(複数選択可)

72.0%の企業が「バックアップ対象毎に別々にバックアップ」している。28.7%が「物理サーバ全体をイメージバックアップ」、11.3%が「VM 単位でイメージバックアップ」、5.2%が「ストレージ単位でイメージバックアップ」している(図 4-76)。

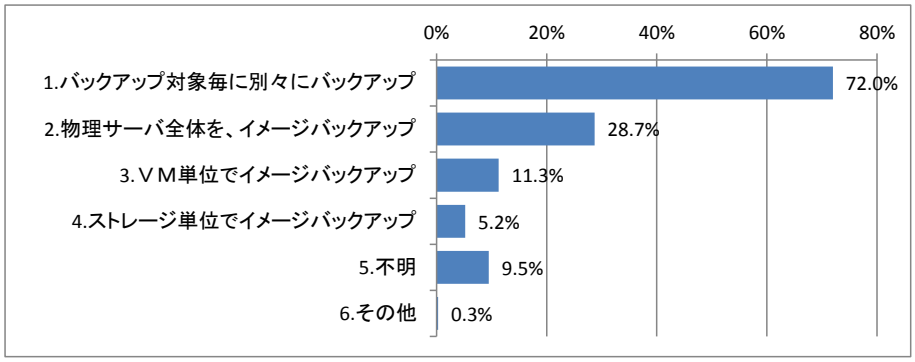


図 4-76　バックアップの実行単位(n=328)

Q33.データの完全性

Q33. データの完全性について教えてください。(一つ選択)

「データの完全性や復旧時のエラー検出に関する要件を定めている」企業は、13.5%となっており、「定めていない」とするそれ以外の企業は 67.8%となっている(図 4-77)。データの完全性は、システム復旧時の課題となる場合があるが、この点について意識している企業は未だ少ないと言って良いだろう。

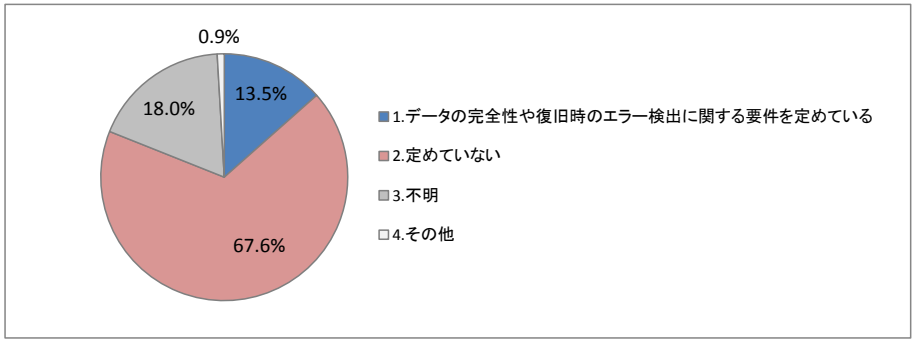


図 4-77　データの完全性(n=327)

Q34.バックアップの方式

Q34. バックアップの方式について教えてください。(一つ選択)

「システムを停止せずにバックアップしている(オンラインバックアップ)」と「オフラインバックアップとオンラインバックアップを組み合わせて実施している」を合わせると、オンラインバックアップでバックアップを行っている企業が 79.4%となっている(図 4-78)。

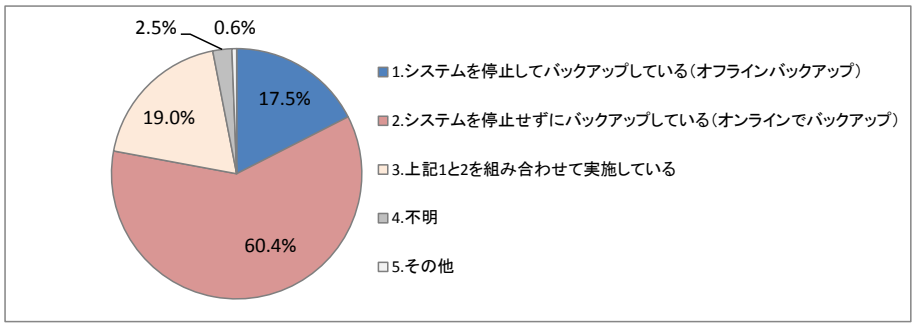


図 4-78 バックアップの方式（n=326）

Q35.バックアップの頻度

Q35. バックアップの頻度について教えてください。（複数選択可）

50.0%の企業が「フルバックアップ（日次）」を行っており、次いで「フルバックアップ（週次）＋日次での差分/増分バックアップ」が 32.8%、「リアルタイムバックアップ」が 17.5%、「フルバックアップ（週次）」と「フルバックアップ（月次）」が 10%程度となっている（図 4-79）。また、本質問は複数選択可としており、1 社あたり平均 1.3 件を選択している。このことから、同一企業であってもシステムによりバックアップ頻度が異なっていることが分かる。

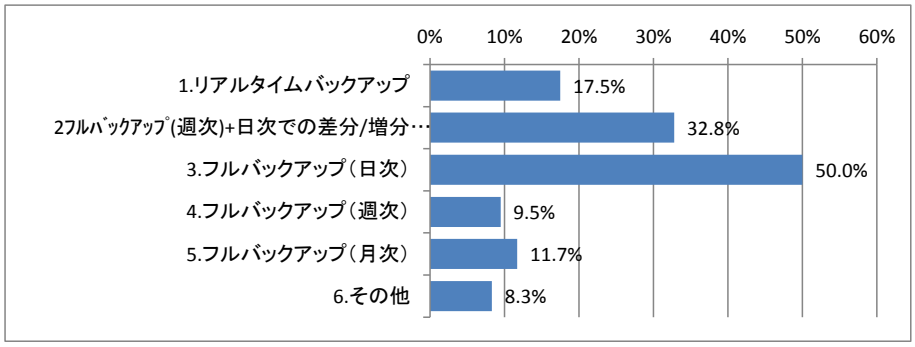


図 4-79 バックアップの頻度（n=326）

Q36.バックアップの世代管理

Q36. バックアップの世代管理について教えてください。（複数選択可）

バックアップデータの世代管理について、「1 世代」までと回答している企業が 24.9%と最も多い（図 4-80）。ただし、「不明」と回答している企業が 23.1%あり、回答者がバックアップの世代管理について十分に把握していないことが推測される。また、本質問は複数選択可としており、1 社あたり平均 1.1 件を選択している。このことから、同一企業であってもシステムによりバックアップの世代管理方法が異なっていることが分かる。

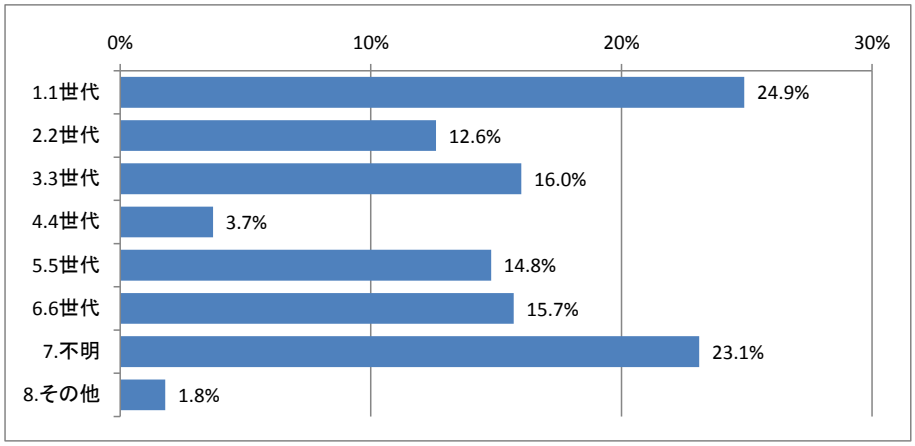


図 4-80　バックアップの世代管理(n=325)

Q37.バックアップしている媒体(メディア)

Q37. バックアップしている媒体(メディア)について教えてください。(複数選択可)

バックアップしている媒体(メディア)は、「磁気テープ」が 54.1%と最も多く、次いで「外付けハードディスクドライブ」、「ストレージ装置」が 35.6%となっていることから、この 3 種類が企業におけるデータ保管のための主な媒体だと考えられる(図 4-81)。

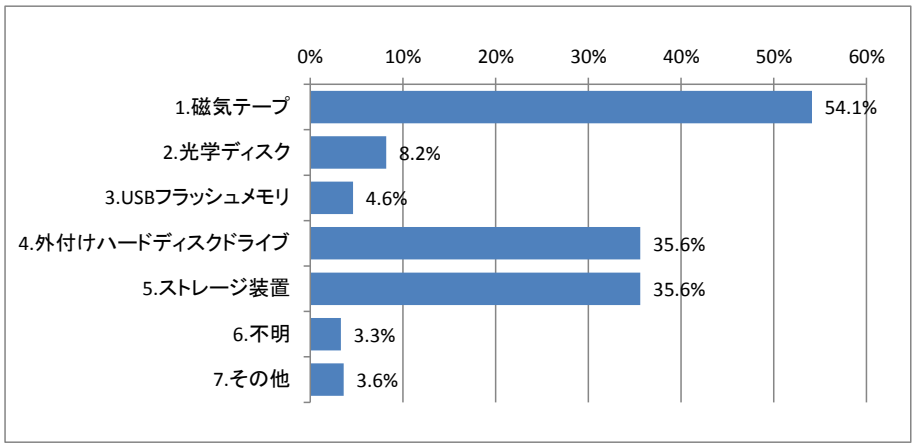


図 4-81　バックアップしている媒体(メディア)(n=329)

Q38.バックアップの保管場所の分散度

Q38. バックアップの保管場所の分散度について教えてください。(複数選択可)

バックアップの保管場所として「本番システムが設置されている拠点と同一拠点」を選択しているのが 74.8%と最も多い。別拠点に保管しているのは、「別拠点(60Km 未満)」と「別拠点(60Km 以上)」とを合わせて 42.2%となっている(図 4-82)。

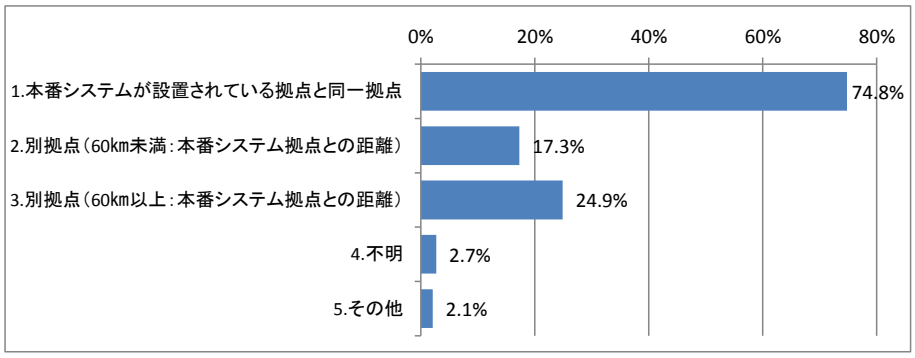


図 4-82　バックアップの保管場所の分散度（n=329）

Q39.異なる拠点でバックアップを保管する場合のバックアップの取得間隔

Q39. 異なる拠点でバックアップを保管する場合のバックアップの取得間隔について教えてください。（複数選択可）

異なる拠点でバックアップを保管している企業のうち、「非同期（日次）」でバックアップデータを取得する企業が 45.7%と最も多く、次いで「非同期（週次）」が 25.2%、「非同期（月次）」が 20.5%、「リアルタイム」が 14.2%となっている（図 4-83）。

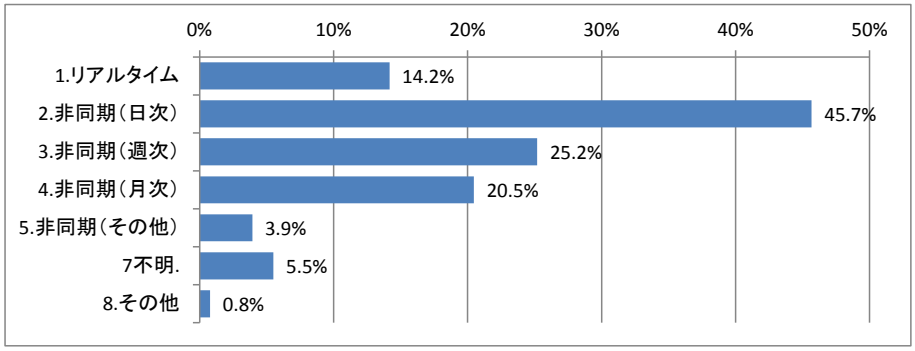


図 4-83　異なる拠点でバックアップを保管する場合のデータの取得間隔（n=127）

Q40.バックアップデータの施錠管理状況

Q40. バックアップデータの施錠管理状況について教えてください。（複数選択可）

バックアップデータの施錠管理状況として「保管している部屋に施錠」している場合が 40.5%と最も多く、次いで「保管している建物に施錠」が 28.7%、「保管している筐体（棚・耐火金庫等）に施錠」が 28.3%となっている（図 4-84）。なお、施錠対象は、1 企業あたり平均 1.4 件となっている。

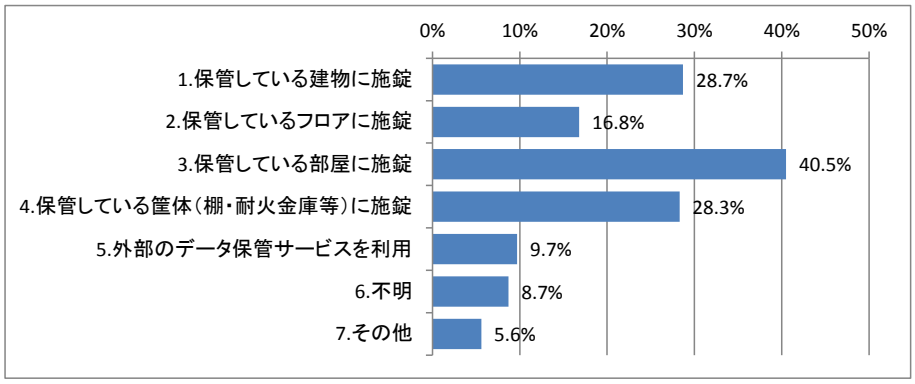


図 4-84 バックアップデータの施錠管理状況(n=321)

Q41.バックアップデータの暗号化

Q41. バックアップデータの暗号化状況について教えてください。(一つ選択)

バックアップデータの「全てを暗号化している」および「一部を暗号化している」と回答した企業は22.5%となっている(図 4-85)。バックアップデータの暗号化は、データの機密性を確保する上で有効な対策であるが、現状では暗号化を行っている企業は少数派である。

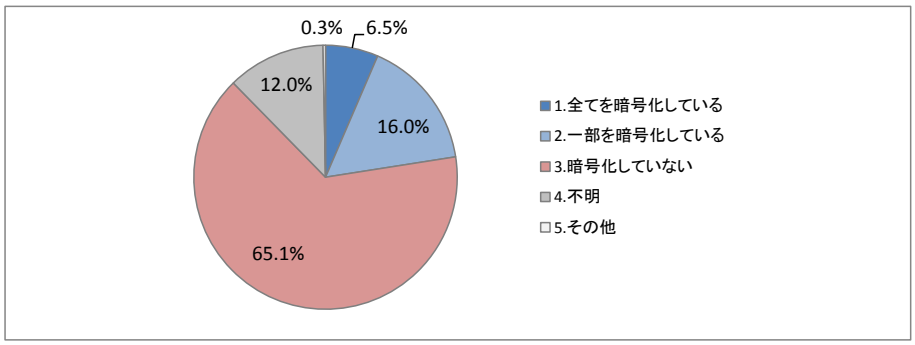


図 4-85 バックアップデータの暗号化(n=324)

Q42.バックアップ作業の自動化の範囲

Q42. バックアップ作業の自動化の範囲について教えてください。(一つ選択)

「全てのバックアップ作業を自動化している」および「一部のバックアップ作業を自動化している」と回答した企業は 82.2%となっており、バックアップ作業を手動のみで実施している企業は少数派である(図 4-86)。

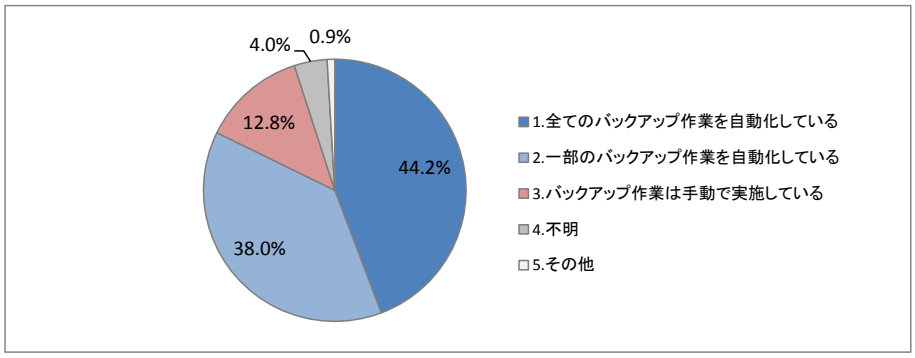


図 4-86 バックアップ作業の自動化の範囲(n=321)

⑦ 震災被害の経験とその後の対応

東日本大震災等の震災被害の経験とその後の対応について、データの保管(バックアップ)対策の観点でたずねた。

Q43.情報システムの利用を制限された経験のある震災

Q43. 情報システムの利用を制限された経験のある震災について教えてください。(複数選択可)

情報システムの利用を制限された経験のある震災についてたずねたが、62.8%は「経験はない」と回答した。利用を制限された経験のある震災は、「東日本大震災[2011.3]」が 29.3%と最も多く、次いで「阪神大震災[1995.1]」が 6.2%と続いた(図 4-87)。なお、「その他震災」には、震災とは直接関係ないものの、台風や大雨、送電線損傷事故等が挙げられている。

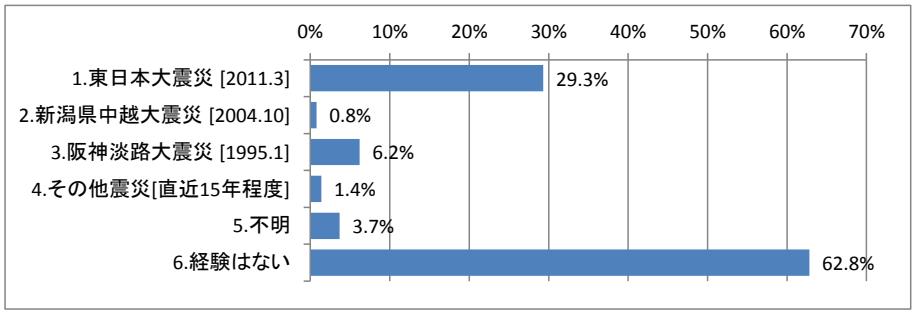


図 4-87 情報システムの利用を制限された経験のある震災(n=355)

Q44.東日本大震災等の震災後の、データの保管(バックアップ)に対する認識の変化

Q44. 東日本大震災等の震災後の、データの保管(バックアップ)に対する認識の変化について教えてください。(一つ選択)

「震災前の対策では不十分だと認識し、対策の検討を開始した」企業は 35.0%、「震災前の対策では不十分だと認識したものの、対策の検討には至らなかった」企業は 28.2%となった。それ以外の企

業は、震災をきっかけとした対策の見直しは行っていない（図 4-88）。

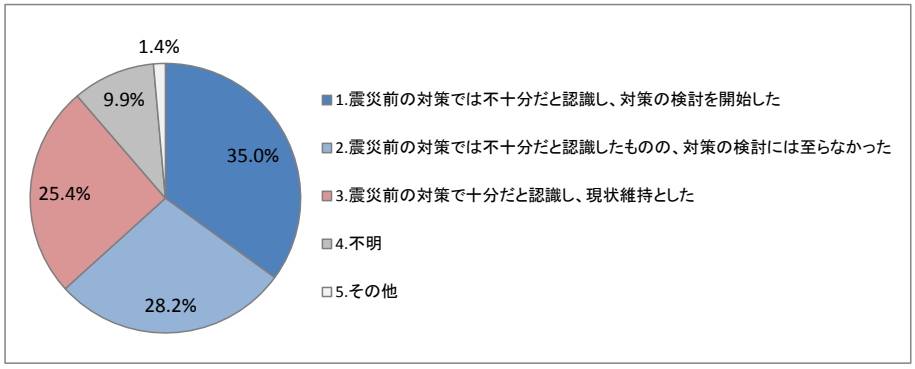


図 4-88 東日本大震災等の震災後の、データの保管（バックアップ）に対する認識の変化（n=354）

Q45.震災で経験したまたは今後懸念する、データの保管（バックアップ）に関する被害や問題

Q45. 震災で経験したまたは今後懸念する、データの保管（バックアップ）に関する被害や問題について教えてください。（複数選択可）

震災で経験したまたは今後懸念するデータの保管（バックアップ）に関する被害や問題は、「メインサイトのシステムのデータの滅失」が 72.6%と最も多く、次いで「バックアップ（データ）の滅失」が 56.5%、「バックアップの復元に時間がかかる」が 52.4%、「メインサイトのシステムのソフトウェアの滅失」が 45.2%となっている（図 4-89）。

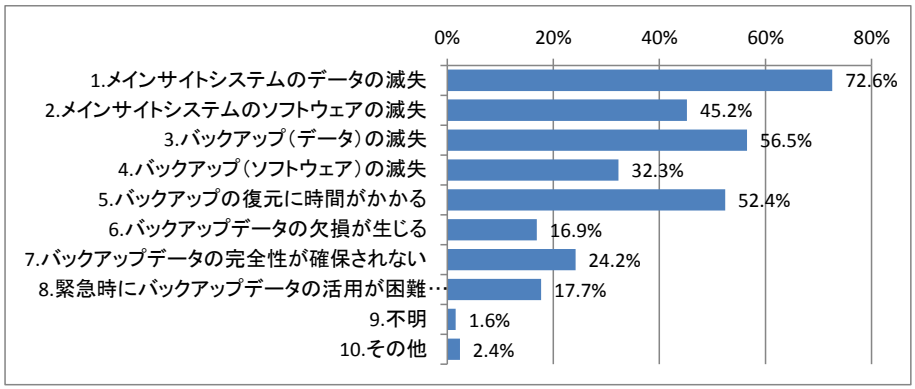


図 4-89 震災で経験したまたは今後懸念する、データの保管（バックアップ）に関する被害や問題（n=124）

Q46. 震災後に検討を開始したデータの保管（バックアップ）に関する対策

Q46. 震災後に検討を開始したデータの保管（バックアップ）に関する対策について教えてください。（複数選択可）

震災後に検討を開始したデータの保管（バックアップ）に関する対策として、「バックアップの保管

場所の分散度の見直し」が 43.5%と最も多く、対策の検討を行った企業の半数近くが挙げている。次いで、「バックアップ方式の見直し」が 39.5%、「バックアップポリシーの策定や見直し」と「バックアップ対象の見直し」が 33.1%となっている(図 4-90)。

具体的なソリューションとしては、遠隔バックアップ用アプライアンスの導入、重複排除機能を利用したバックアップデータの遠隔地保管の実施、東京-大阪間でのストレージレプリケーションの実施、などが挙げられている。

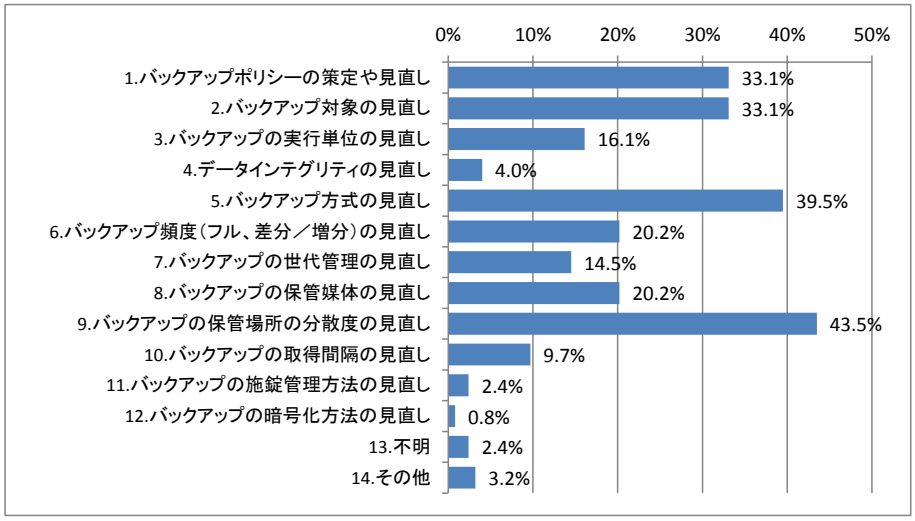


図 4-90 震災後に検討を開始したデータの保管(バックアップ)に関する対策(n=124)

⑧ その他復旧に関する事項

東日本大震災等の震災に関わらず、過去に経験した復旧に関する事項についてたずねた。

Q47.過去に、システムの復旧において、問題となった事項

Q47. 過去に、システムの復旧において、問題となった事項について教えてください。(複数選択可)

過去にシステムの復旧において問題となった事項は、「復旧手順が未整備」が 21.4%と最も多く、次いで「必要なデータの消失」が 20.4%、「電源の確保ができなかった」が 19.5%、「通信を確保できなかった」が 16.9%となっている(図 4-91)。「その他」では、「アプリケーションの更新プログラムを管理できておらずシステム再構築に時間を要した」、「平常時より、システムで利用するデータを物理媒体で搬送していたが、東日本大震災の際に道路状況が悪化したことにより、期日どおりにデータを入手することが危ぶまれた」などが挙げられている。

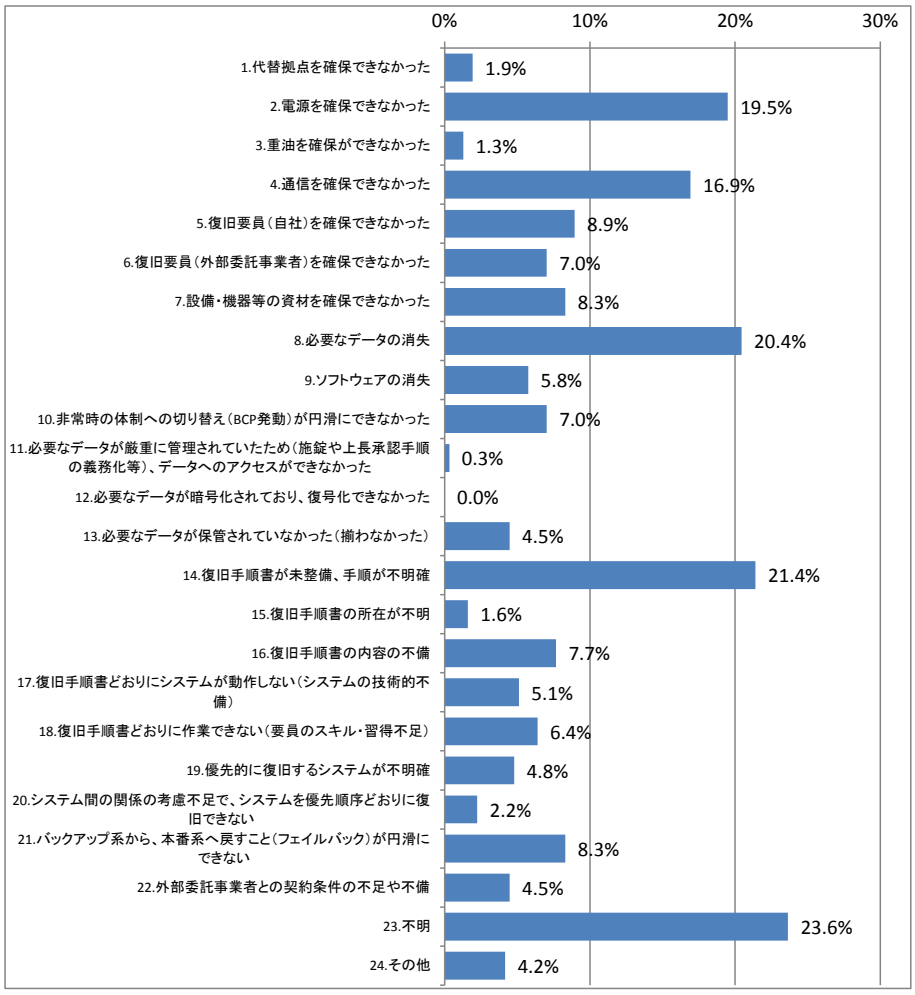


図 4-91 過去に、システムの復旧において、問題となった事項(n=313)

Q48.システム復旧に有効であった技術・サービス

Q48.システム復旧に有効であった技術・サービスについて教えてください。(複数選択可)

システム復旧に有効であった技術・サービスとして、「データセンタ」が 42.6%と最も多く挙げられており、次いで「仮想化技術」が 29.0%、「クラウドサービス」が 14.8%、「無線等を使った通信サービス」が 10.3%となっている(図 4-92)。「その他」では、「専門業者によるデータのサルベージ」、「バックアップ電源(設備電源切替システムへ)」等が挙げられている。また、技術・サービスに該当しないものの、「マンパワー」、「詳しい社員」といった人的要素が有効であるとする回答もあった。

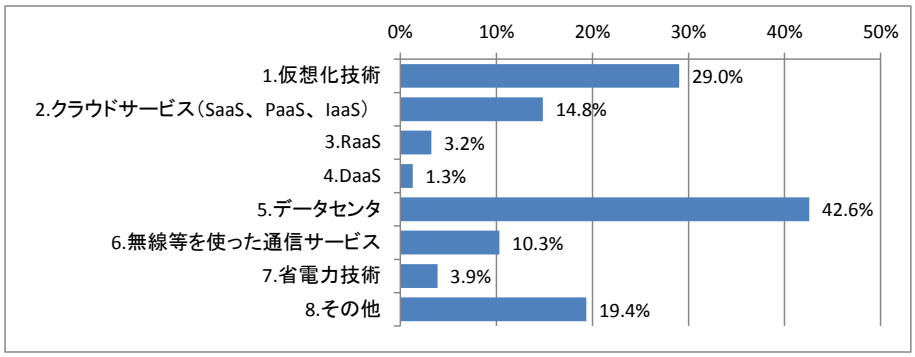


図 4-92 システム復旧に有効であった技術・サービス(n=155)

4.1.3 アンケート調査のまとめ

(1) IT サービス継続に対する意識や平常時の準備や活動

- BCP を「策定済み」とした企業は 40.1%、「未策定(検討中)」は 33.1%。IT-BCP を「策定済み」とした企業は 24.8%、「未策定(検討中)」は 40.9%。事業規模や IT 依存度が大きくなるほど BCP と IT-BCP を策定している傾向が高い。事業規模が大きくなるほど事業の IT 依存度が高まり、結果的に BCP や IT-BCP の必要性が高くなると考えられる。
- 「事業継続のために必要な IT サービスを特定」している企業は 52.2%。一方、「BIA の実施(25.0%)」や「IT サービスの目標復旧時間を策定(28.1%)」、「教育訓練計画を策定(19.7%)」、「事後対策計画を策定(29.8%)」、「維持改善計画を策定(17.1%)」の割合は、IT サービスの特定と比較して相対的に低い。文書の作成だけでなく、充分な戦略の策定や教育訓練、継続的な見直しが重要である。
- IT サービス継続策定時に想定するリスクは、上位から「自然災害(直下型地震による局所被害)」、「自然災害(大規模地震による広域災害)」、「停電」、「ハードウェアの故障」、「通信回線関連の故障」、「建物や施設の破壊・損失」の順となっている。業種別では、金融業が他の業種と比較して多様なリスクを想定する傾向にある。
- IT サービス継続に関して重点的に取り組んでいる領域は上位から「冗長化された電源供給やネットワーク」、「データの遠隔地保管」、「情報処理設備や機器の冗長化」、「耐震構造の建物やバッ

クアップサイト」、「システム運用の仕組みや体制」、「OS 等やデータの冗長化」の順となっている。
・復旧対策に有効だと言われる IT-BCP が多くの企業で策定されていないことは今後の課題であり、その実態を踏まえた対策が必要である。

(2) コンピュータシステムと新しい技術の採用状況

・「事業継続において最も重要なシステム」は全業種で共通して「財務会計システム」や「人事・給与システム」を挙げる企業が多い。業種毎では、製造業が「生産管理システム」を多く挙げるなど、業種の特徴により重要システムが異なる傾向がある。
・事業継続において重要なシステムと、データの保管がなされているシステムは概ね同様であるが、必ずしも一致しない。
・仮想化とクラウドの利用には相関がある(クラウド利用の仮想化導入率は 54.0%、クラウド未利用の仮想化導入率は 21.2%)。
・クラウドサービスの導入目的は、利用中企業と検討中企業との間で上位 3 つの項目は同様であるものの、順番が異なることから、期待と実際が異なっていることがうかがえる(利用中企業は、「運用費用の低減」、「導入費用の低減」、「災害への対策」の順になっている。検討中企業は「災害への対策」、「運用費用の低減」、「導入費用の低減」の順となっている。)。
・SaaS 以外の PaaS や IaaS といったクラウドサービスは、これからの普及が期待される。

(3) システム構成

・事業継続に最も影響の大きいシステムにおいて、待機系システムが設置されているシステムは全体の 52.8%、遠隔にも待機系システムを設置しているシステムは 15.3%となっている。
・資本金の額、拠点数、従業員数、IT 依存度の高さに応じて、システムを冗長化している傾向が強い。特に金融業はバックアップサイトを設置している割合が他の業界と比較して高い。
・大規模障害や大規模災害に対応できる対策を実施している企業は少なく、それらのリスクを想定した対策の充実が必要である。

(4) リカバリ要件定義の有無(事業継続に最も影響の大きいシステムについて)

・事業継続に最も影響の大きいシステムにおいて、目標復旧時間(RTO)／目標復旧レベル(RLO)／目標復旧時点(RPO)を策定している企業は2割程度にとどまっている。BCP、IT-BCP を策定している企業ほどリカバリ要件定義を策定している割合が高い。IT 依存度の高さとの相関が見られる。IT 依存度の高さを認識している企業ほど、復旧に関する具体的な目標に基づき対策を実施していることが推察される。
・IT サービス継続に関する取り組み(ビジネスインパクト分析(BIA)の実施、事前対策、対策実施計画、教育訓練計画、維持改善計画)の実施状況別に、事業継続に最も影響の大きいシステムにおける目標復旧時間(RTO)の策定状況をみると、各取り組みを実施している企業の方が、目標

復旧時間（RTO）を「策定済み」としている割合が高い。一般的に、共通の目標は、複数の関係者同士が協力して取り組みを推進する場合に重要な役割を果たすことから、複数部門が関連するIT サービス継続の取り組みにおいては、目標復旧時間（RTO）等の具体的な指標が、共通の目標として重要な役割を果たしていると推察される。

・事業継続に最も影響の大きいシステムにおける目標復旧時間（RTO）で最も多いのは、「1～6 時間」。目標復旧レベル（RLO）で最も多いのは「障害・被災前と同等の業務を実施できる水準」。目標復旧時点（RPO）は、「障害・被災発生の前日まで復旧」が最も多い。

・目標復旧時間（RTO）毎に企業をグルーピングし、それぞれのシステム冗長化状 況を確認したところ、目標復旧時間（RTO）が 6 時間未満のグループであっても、 システムの冗長化を行っていない企業が、各グループで 15%～25%程度あった。事業継続性を確保するためには、IT サービス継続戦略と対策の整合性を確保しておくことが重要である。

・復旧対策に RTO が有効に機能していると考えられることから、RTO を活用した対策が重要である。

(5) データの保管（バックアップ）の実施状況（事業継続に最も影響の大きいシステムについて）

・バックアップを実施している企業は 92.7%となっている。

・バックアップポリシーを全部または一部のシステムで明確化している企業は 71.0%となっている。

・バックアップポリシーを明確化していない 26.1%の企業のうち、59.3%は IT 依存度が高い（「ほとんどの事業、業務が IT に大きく依存している」と「IT に依存している事業、業務が多い」の合計）としている。IT 依存度が高いにも関わらず、バックアップポリシーが明確化されていない場合、適切な復旧目標を検討できない可能性が考えられる。バックアップポリシー明確化の有効性についての認知度を向上させる取り組みは、社会的な復旧力を向上させる上でも重要な取り組みになると考えられる。

・バックアップデータは 36.1%が別拠点に保管しており、52.9%がシステム設置拠点と同一の拠点のみに保管している。ただし、「ほとんどの事業、業務が IT に大きく依存している」とする企業であっても、別拠点に保管している割合は 49.5%にとどまっている。

・データの保管（バックアップ）対策は、資本金規模や IT 依存度が高まるに連れ、充実している傾向が強い。事業規模が大きくなるにしたがい、事業における IT の位置づけが大きくなり、結果的にデータの保管対策が充実していることが推察される。

・IT 依存度に応じたデータ保管対策の実施が重要である。

(6) 震災被害やその他の障害の経験とその後の対応

・情報システムの利用を制限された経験が最も多いとされた震災は、東日本大震災である。

・「震災前の対策では不十分だと認識し対策の検討を開始した」企業は 36.2%、「震災前の対策では不十分だと認識したものの、対策の検討に至らなかった」のは 27.6%、「震災前の対策で十分だ

と認識し、現状維持とした」のは 25.9%となっている。自らの経験により必要性を実感した企業は、データが毀損・滅失することを、より切実な問題として捉えていると考えられる。

・ データのバックアップに関する被害や問題として、「メインサイトシステムのデータの滅失」や「バックアップ（データ）の滅失」、「バックアップの復元に時間がかかる」が上位に挙げられている。

・ 震災後に検討を開始したデータのバックアップに関する対策には、「バックアップの保管場所の分散度の見直し」、「バックアップ方式の見直し」、「バックアップポリシーの策定や見直し」、「バックアップ対象の見直し」が上位に挙げられている。

・ 過去にシステムの復旧において問題となった事項として、電源や通信の確保ができない等のインフラに関する事項のほか、必要なデータの消失や復旧手順書の不備といった対策・運用に関する事項が挙げられており、これらに関する対策が重要である。

これまで見てきたように、企業等におけるデータ保管等に関わる取り組みの実態が明らかになった。全体として、事業規模や事業の IT 依存度が大きいほど、対策が充実している傾向がうかがえたものの、復旧目標に対して十分な対策が取られていない例が散見された。今後はシステム復旧目標に合わせた対策の充実が望まれる。

4.2 対策の実施状況

4.2.1 ヒアリング調査の概要

企業の IT サービス継続マネジメントの取り組みを検討・実施していく際には、システム復旧対策を実施している企業等の実践事例が参考になる。そこで、企業、地方公共団体に対してヒアリング調査を実施した。調査の概要は表 4-7 に示すとおりである。

表 4-7 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企業における 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、企業が 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 11 組織	
調査項目	①事業の特徴と IT	企業の IT の活用状況や IT ガバナンスの取り組みを調査する。
	②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内容や検討方法を調査する。
	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を調査する。
	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、留意点を調査する。
	⑤システム復旧対策の詳細	情報システム基盤の復旧対策の詳細を調査する。
調査時期	2012 年 4 月～5 月	

4.2.2 個別事例の紹介

今回調査を実施したのは、表 4-8 に示す企業、地方公共団体である。

表 4-8 ヒアリング調査の対象

主なシステムのタイプ	企業等	最重要システム	業種	対策の特徴
外部向けオンラインシステム	A 社	検査・認証情報データベース	サービス業	・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、震災時に切り替え処理を実施。
	B 社	決済代行システム	サービス業	・システム障害対策のため、メインサイトの冗長化、回線の三重化を実施。
	C 社	Web サービス（情報提供）、ブロガーを管理するプライベート SNS	サービス業	・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。
	D 社	基幹システム	金融・保険業	・システム障害対策のため、メインのサーバは三重化を実施。
外部向け窓口システム	E 団体	住民基本台帳システム等	地方公共団体	・東日本大震災時に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。
内部向けシステム	F 社	製造・販売・管理システム、メール、CTI システム等	製造業	・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。
	G 社	生産管理システム等	製造業	・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。
	H 社	メールシステム、顧客用開発システム（ファイルサーバ）等	サービス業	・遠隔地にオンラインバックアップ。一部テスト機を活用した冗長化を実施。
	I 社	ERP、メール・グループウェアシステム	サービス業	・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。
	J 社	契約者情報管理システム	その他	・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。
	K 団体	IT 基盤システム（全庁ネットワーク LAN、WAN、認証基盤、メール・グループウェア、ファイルサーバ、公開用 Web サーバ等）	地方公共団体	・IT-BCP（地震対策）を策定し、IT 基盤を優先した冗長化対策を実施。 ・住民基幹系システムは遠隔地バックアップを実施。

(1) A 社

① 企業の事業の特徴と IT

a. 業種・企業概要

・ 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

b. 全社レベルの IT ガバナンス

＜IT の活用＞
・ 検査や認証等の管理業務を実施する上で、その情報を管理し、顧客に提供するために、IT はなくてはならないものとなっている。

＜IT の活用を促進する推進体制＞
・ IT に関することは国内情報システム部門長が検討し、CIO(海外)と協議して決定する。IT ディザスタリカバリプラン(緊急時対応計画)もこの体制で策定している。対策の実装は情報システム部門が実施している。

c. BCP の策定とマネジメント

＜震災による変化等＞
・ 震災を契機に、BCM(事業継続マネジメント)に関する取り組みを行うこととなった。震災以前は、1つの重要なサービスを除いて BCM に関する手順は策定されていなかった。
・ BCM は、事業を継続するための取り組みであり、リスク全般を包含する。一方、BCP や IT ディザスタリカバリプランは事象が発生した際の対応を策定するものであり、事業保全のための取り組みであると位置づけている。

＜BCP 策定体制＞
・ BCP/BCM は、BCP 所管部門が担当している。BCP 担当で検討し、社長と協議して決定する。

＜BCP の策定手順＞
・ BCM を行う上で、ビジネスインパクト分析(BIA)を重視している。当初、社長からは、すべての事業を対象としてビジネスインパクト分析(BIA)を行うよう指示があったが、特に売上の高い事業と、重要な顧客サポート業務を優先して対象範囲を決定した。
・ ビジネスインパクト分析(BIA)では、各業務プロセスにおいて、各工程や処理がどのように関連しているのかを分析している。たとえば、営業担当者が見積もりを提出する際には、訪問、電話、FAX のようなコミュニケーション手段をどのように利用しているか、見積り様式の選定方法や選定内容、システムの利用有無などを分析する。このように、業務フロー、物品等の資源、組織・人材などについて詳細なレベルで検討を行っている。業務部門の担当者に対して事業継続の考え方

から説明し、1～3 か月程度を掛けて実施してもらっている。
・ビジネスインパクト分析（BIA）の作業は負担が大きいが、実際に被災したときに発生する損害を考えると、それに対する備えとして、無駄にはならないと考えている。
・BCM やISMS などのマネジメントシステムは、別々で構築してきたが、最終的に統合する方向で構築・運用する方が良いと考えられる。

＜BCP 策定体制＞

・BCM の策定には、社長、副社長、CXO（Chief X Officer：各分野の責任者）が関与し、全社的に取り組んでいる。

＜教育訓練＞

・新規に配属された従業員にはその都度、当社の BCP、BCM に関する考え方説明を行っている。
・全拠点で、BCP において緊急時の手順が策定されており、保存している。各拠点とも同様の手順ではあるが、地理的条件が異なるので、その点だけ内容が異なっている。

＜対象リスク＞

・リスクはビジネスインパクト分析（BIA）を通じて評価しており、個別リスクの発生確率よりもリスクによって生じるインパクトを重視している。

d. IT サービス継続計画（IT-BCP）の策定とマネジメント

＜IT-BCP の策定状況＞

・情報システム部門が中心となって、IT ディザスタリカバリプランを以前から策定していた。
・10 年ほど前に情報システム部門においてIT ディザスタリカバリに関する技術的な手順を策定した。当時は、現在ほど組織は大きくなく、簡単な手順が示されている程度だった。
・IT ディザスタリカバリに関して、システム単位での導入計画はあるが、全社的な導入計画は無い。また、緊急時対応の考え方はあるが、BCM の考え方はまだ含まれていない。BCP 策定にあわせて、BCP と連携した IT-BCP を策定しているところである。
・新しいシステムが導入される際には、IT-BCP の観点での研修を行っている。

＜IT-BCP の策定体制＞

・IT ディザスタリカバリは、情報システム部門が担当している。IT に関することは国内情報システム部門長が検討し、CIO（海外）と協議して決定する。

② 企業の重要業務と継続戦略

a. 重要業務

・最重要業務は、検査や認証等の管理業務である。
・構築している情報システム基盤には、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。

b. 業務選定の理由・経緯

・IT ディザスタリカバリプランにおいて、システムの優先順位づけは決定されている。もっとも重要な業務は顧客への情報の提供（オンラインのデータベースサービス）である。具体的には、認証済み製品に対し認証済みであることを証明するために付与するユニークな認証番号により、情報を提供するサービスである。この情報がないと、顧客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。

c. 戦略の内容と検討方法

［目標復旧時間（RTO）］

・目標復旧時間（RTO）は、もっと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 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、もっとも高水準のもので 5 分と設定した。

［目標復旧レベル（RLO）］

・特に設定していない。

［目標復旧時点（RPO）］

・特に設定していない。

・このような内容は、社長は直接判断に関与しない。情報システム部門は、事業部門からの要求に基づいて対策を検討して、予算の範囲で対応する。

③ 重要業務のためのシステムの概要

a. 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。

b. 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の専用回線で結ばれ、最短5分でデータをコピーしている。

・ストレージベースのレプリケーション機能のおよび、仮想化技術（災害対策機能）を活用し最短 5 分で切り替え可能。

・システム構成の概要を図 4-93 に示す。

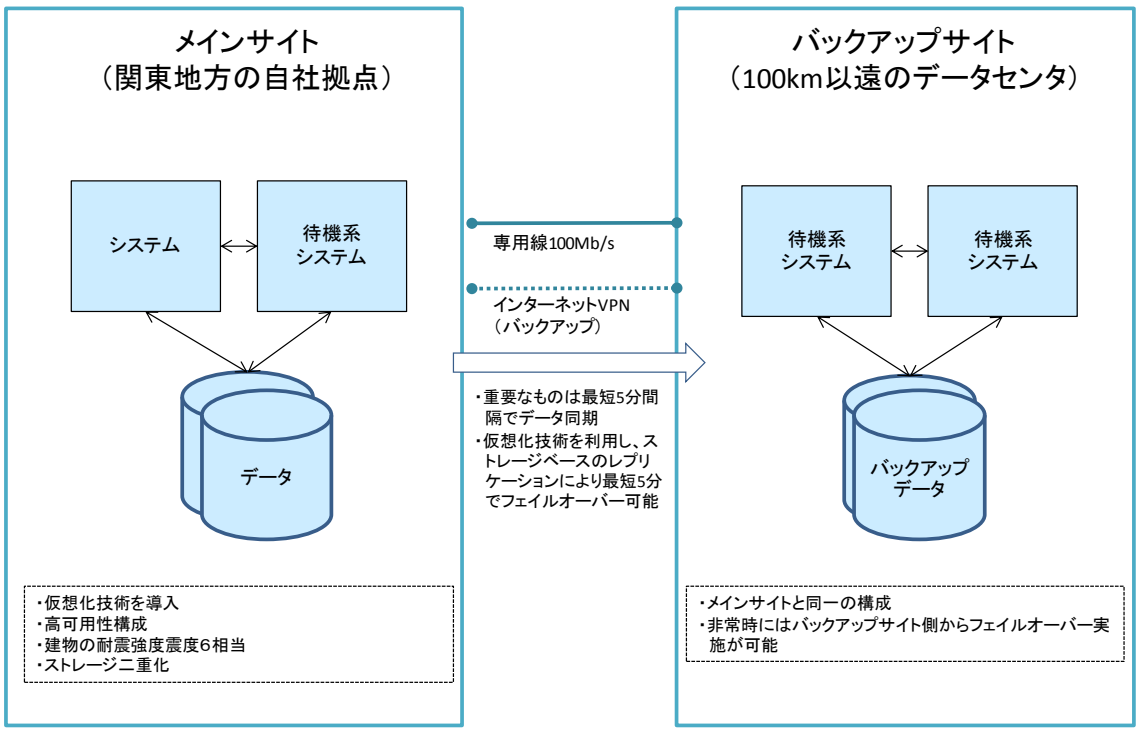


図 4-93 システム構成の概要

＜この構成を採用した理由や判断基準＞

・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っている。現在の構成に変更することにより、システム復旧対策を実現するとともに、コストが削減された。

・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で各 1 名ずつである。以前は各ロケーションに分散していたので、運用要員が 5～6 人必要だった。また、サーバ台数も縮減できた。

・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。

＜対策の概算費用＞

・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。

c. 技術的特徴

＜導入した技術・サービスの内容＞

・仮想化技術を導入している。

・ストレージベースのレプリケーションを実施している。

＜導入メリット＞

・サーバ集約を図ることにより、コストの削減とバックアップサイトの構築を両立できた。

・レプリケーション機能および、仮想化技術（災害対策機能）による短時間でバックアップサイトへの切り替えが実現できた。

④ システム復旧対策のポイントと留意点

a. 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に、150VM 中、15VM を切り替えた。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。

・通常運用形態へ戻す処理には 2 週間ほど要した。データの最新化に時間を要したためである。当時は、通常運用形態へ戻す処理の経験や標準手順が確立してなかった。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、戻す処理の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。

b. ポイント

・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。

c. 留意点や将来構想

＜将来構想＞

［バックアップサイトについて］

・今後、災害時、バックアップサイトの起動は、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。

［マネジメントシステムの構築］

・震災を受け、BCM 全体を再構築している。

・全社的なビジネスインパクト分析（BIA）を実施するとともに、IT-BCP と連携したマネジメントシステムを構築している。この中には ISMS も取り込んでいる。

＜留意点＞

・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考えている。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。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-9 のとおりである。

表 4-9 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		目標復旧水準（業務停止時）	RPO（目標復旧時点）	未設定
			RTO（目標復旧時間）	5 分
			RLO（目標復旧レベル）	未設定
		目標復旧水準（大規模災害時）	システム再開目標	1 日以内
	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）
			冗長化（コンポーネント）	全てのコンポーネントを冗長化
		ネットワーク機器	冗長化（機器）	全ての機器を冗長化
			冗長化（コンポーネント）	電源・FAN 等は冗長化されている
		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
			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
		ストレージ	冗長化（機器）	ストレージ 2 台構成
			冗長化（コンポーネント）	一部のコンポーネントを冗長化
			冗長化（ディスク）	RAID-DP による冗長化
		データ	バックアップ方式	オンラインバックアップ
			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
	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
		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
			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
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
			監視間隔	リアルタイム監視（1～2 分間隔）
	保守運用	定期保守頻度	定期保守頻度	年 1 回
		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
	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
		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
			駆けつけ到着時間	原則 3 時間以内
			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
		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
			予備機の有無	ブレードサーバの予備機が有り
	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
	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
		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
		オペレーション訓練	オペレーション訓練範囲	非回答
		定期報告会	定期報告会実施頻度	非回答

大項目	中項目	小項目	指標	対策
			報告内容のレベル	非回答
システム環境	機材設置環境条件	耐震/免震	耐震震度	建設は 1981 年以降なので、震度 6 強にも耐えられる
		電気設備適合性	停電対策	非回答

(2) B 社

① 事業の特徴と IT

a. 業種・企業概要

・ 業種:サービス業

・ 業務内容:クレジットカード決済代行業務

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞

・ システムで提供するサービスそのものが業務であるため、システム依存度は非常に高く、経営戦略との関連も高い。

＜IT 投資の比率＞

・ IT 支出(ハードウェア購入・ソフトウェア開発費)は平成 23 年度ベースを例とすると、売上全体の 15%程度である。

＜IT の活用を促進する推進体制＞

・ IT の企画全般を担当しているのが事業部門長である。業界のセキュリティ基準に基づき、カード会社側の要請など世の中の変化やニーズに応えていくことができるよう対応してゆくことに主眼においている。CIO に相当する位置づけとなるのは、システムの運用責任者となる部長であり、システムの運営全般を総括している。

c. BCP の策定とマネジメント

＜BCP 対応方針について＞

・ BCP という名称の資料は無い。当社を含むグループ会社全体としては緊急時の対応計画はある。当社においては、復旧手順等について、運用マニュアルの中に含めている。運用マニュアルは運用責任者となる部門長が管理しており、記載内容については経営層にも報告されている。

d. IT サービス継続計画(IT-BCP)の策定とマネジメント

＜IT-BCP の構成＞

・ BCP と、IT-BCP の分離はできない。

＜策定時期、見直しの頻度＞

・ サービスを開始した当初から運用マニュアルを策定してきたが、定期的に年 1～2 回見直しを行うとともに、新しいソフトウェア・ハードウェアを導入する際には随時更新している。また、トラブル発生における教訓や顧客からのクレームによっても内容を見直している。

＜対象リスク＞

・ 地震、火事、雷、ハードウェア故障(特に電源・通信回線の停止による影響は大きい)

＜教育訓練や演習の実施と内容＞

・定期的に業界のセキュリティ基準に準じて訓練を行っている。

・教育内容としては、機器を維持するのに必要な知識の共有や故障時の操作等を行っている。緊急連絡網も当然備えており、日常的に連絡を取り合う際に利用している。

・復旧訓練は年 1 回実施しており、火災を想定した訓練を実施している。予備電源などを使用し、停電を想定した訓練も行っている。訓練とは別に、技術的な面では座学や勉強会などを行っている。

e. 震災の影響

・業界のセキュリティ基準への具体的な対応策を実装中だったので、震災を機に対応を更に推進することとした。

・マシン類をデータセンタに預ける検討はしたが、予算化するところまでの具体的な対策案とはなってない。

② 重要業務と継続戦略

a. 重要業務

＜選定した重要業務＞

・クレジットカード決済代行業務

b. 業務選定の理由・経緯

＜選定の理由や判断基準＞

・会社の提供する唯一のサービスである。

＜戦略検討の方法＞

・経験則に基づき停止時間の上限を設定している。夜間は利用者が少ないが、夜間にシステムが停止した際にもクレームが発生したことがあったため、昼間と同等の目標値とした。

＜設定した目標＞

[目標復旧時間(RTO)]

・ハードウェア故障時は数分以内で復旧。

[目標復旧レベル(RLO)]

・外部へサービス提供している全システムを対象とする。

[目標復旧時点(RPO)]

・障害発生直前まで復旧する。確定したトランザクションは保証する。

③ 重要業務のためのシステムの概要

a. 規模

・サーバ 20 台程度

・利用者は不特定多数

b. システム構成と復旧対策の概要

・メインサイト内でシステムは 2 重化し、故障発生時は自動的に待機系システムに切り替わる。

・本番機から待機系システムへは、リアルタイムにバックアップを実施である。

・トランザクション実行中に待機系システムに切り替わった場合、救済措置を手動で実施している。これには 30 秒程度を要する。

・バックアップの外部保管は未実施である。

・CAFIS と接続するネットワークは三重化している。ユーザ企業と接続するネットワークは二重化している。

・システム構成の概要を図 4-94 に示す。

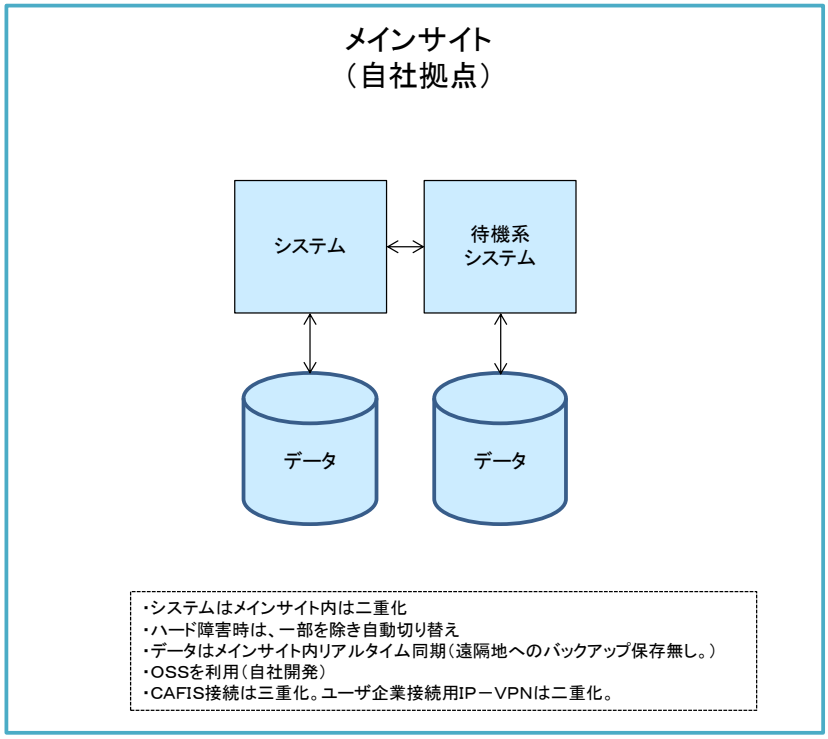


図 4-94 システム構成の概要

＜この構成を採用した理由や判断基準＞

・顧客の要望に応え、ハードウェア故障時の切り替えを最短に留めるような構成としている。過年度において継続的に改善を加えた結果、現在の構成となった。

・キャパシティプランニングに必要なトランザクション予測も影響を与える。顧客から、カード決済機器配備の拡張プランを入手し利用箇所の全体数は把握している。また、顧客から提供を受けるデータや、シンクタンク等が公表しているクレジットカード利用額の推計値などを参考に試算している。

c. 技術的特徴

＜ポイント＞

・ハードウェア故障時の切り替えをできるだけスムースに実施するため、市販のミドルウェアはできるだけ使用せず、ソースが開示されているオープンソースソフトウェア（OSS）を用いて、レプリケーションやサーバ冗長化を行っている。各自が OSS を改造できるレベルまで従業員の技術レベルは習熟している。

④ システム復旧対策のポイントと留意点

a. 震災時等の効果

・直接の影響は無かった。

b. ポイント

・経営陣と従業員の課題共有を実施できている。特に、顧客からのクレームに関する情報が共有されており、クレーム対策がシステムの継続的な改善に結びついている。

c. 留意点や将来構想

・業界のセキュリティ基準対応では代替策を採用している事項もあり、それらを再検証、改善することが優先課題のひとつである。

・中期的にはバックアップサイトを構築しバックアップすることを検討していく必要があると考えている。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-10 のとおりである。

表 4-10 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
可用性	継続性	業務継続性	業務継続の要求度	サーバ冗長化構成のため、単一障害では業務停止しない
		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）
			RTO（目標復旧時間）	数分と設定している
			RLO（目標復旧レベル）	全業務を対象としている
		目標復旧水準（大規模災害時）	システム再開目標	数値目標は無い

大項目	中項目	小項目	指標	対策
	耐障害性	サーバ	冗長化(機器)	全てのサーバで冗長化
			冗長化(コンポーネント)	冗長化可能なコンポーネントは冗長化している
		ネットワーク機器	冗長化(機器)	一部冗長化。冗長化できないところは代替機を用意している。
			冗長化(コンポーネント)	非冗長化
		ネットワーク	回線の冗長化	・ユーザとの IP-VPN による接続は二重化している。 ・CAFIS との接続回線は三重化している。
			経路の冗長化	・ユーザ、CAFIS との接続経路は冗長化している。
		ストレージ	冗長化(機器)	ストレージ未使用
			冗長化(コンポーネント)	ストレージ未使用
			冗長化(ディスク)	内蔵ハードディスクについて RAID1 と RAID5 混在
		データ	バックアップ方式	オンラインバックアップ
			データインテグリティ	不明
	災害対策	システム	復旧方針	災害前と同一の構成を目指すが、優先順位を付けて実施する
		外部保管データ	保管場所分散度	外部保管データはない
			保管方法	同一サイトのハードディスクに保存している。
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している。
			監視間隔	リアルタイム監視(分間隔)
	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)
		予防保守レベル	予防保守レベル	担当者が日々、チェックを行っている
	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	ハードウェア故障時の切り替えは自動。トランザクション救済は手作業
		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
			駆けつけ到着時間	数時間内
			SE 到着平均時間	社員の開発 SE が 24 時間常駐している
		交換用部材の確保	保守部品確保レベル	通常のレベルである
			予備機の有無	ネットワーク機器の二重化できない部分のみ予備機がある
	運用環境	マニュアル準備レベル	マニュアル準備レベル	復旧手順を含めシステム向けにカスタマイズしたマニュアルがある
	サポート体制	一次対応役割分担	一次対応役割分担	一次対応は従業員が実施する
		サポート要員	ベンダ側対応者の要求スキルレベル	ベンダには業務スキルは要求しない
		オペレーション訓練	オペレーション訓練範囲	故障発生時の対応を含めて訓練している
		定期報告会	定期報告会実施頻度	実施していない
			報告内容のレベル	障害報告のみ
システム環境	機材設置環境条件	耐震/免震	耐震震度	阪神淡路大震災以降の建築であり、震度 6 強に耐えられる
		電気設備適合性	停電対策	自家発電装置により、数時間電源確保することができる

(3) C 社

① 事業の特徴と IT

a. 業種・企業概要

・業種:サービス業

・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

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞

・システムで提供するサービスから収入を得ているものもあれば、コンテンツの提供や Web サイト構築等を業務としており、IT の業務関与は高い。

＜IT 投資の比率＞

・IT 関連費用は売上高の 10%程度になる。

＜IT の活用を促進する推進体制＞

・Web サイト構築やサービスに関わる技術担当役員という位置づけで CTO が設置されているが、社内 IT 関連の役割も実質上 CTO が担当している。

・システム関連メンバは 2 名。必要に応じて外部委託もしている。

c. BCP の策定とマネジメント

＜策定時期と見直しの頻度＞

・BCP は作成していない。小規模の会社であり、強力な対策を独自に検討するのは難しい。

＜BCP 対応方針について＞

・IT 以外の人的リソースの面では、属人的な業務を減らし複数人体制に持っていくことは検討課題である。しかしながら、小規模の会社であるため、現実的には困難を伴う。

d. IT サービス継続計画(IT-BCP)の策定とマネジメント

＜策定時期と見直しの頻度＞

・IT-BCP について独立した文書策定の予定は無い。また、いつまでに何をするといった計画があるわけではないが、気付いた都度、様々な規約等に内容を盛り込むよう努力している。

・2009 年に取得した P マーク取得の過程で、情報セキュリティや情報システムのあり様を見直し規定を作成した。その中に、IT-BCP に関わる内容を含めている。

＜教育訓練や演習の実施と内容＞

・復旧手順書自体はある程度は作成している。以前の復旧作業の経験から不備が発見された場合、都度改善はしている。訓練の対象者が自分自身であるケースが殆どのため、有事に対する訓練

は行っていない。

② 重要業務と継続戦略

a. 重要業務

＜選定した重要業務＞

・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

b. 業務選定の理由・経緯

＜選定の理由や判断基準＞

・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。

＜戦略検討の方法＞

・復旧目標値については、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。

＜設定した目標＞

［目標復旧時間（RTO）］

・ハードウェア故障発生時：24 時間以内復旧。

［目標復旧レベル（RLO）］

・ハードウェア故障時：故障発生前と同等の状態へ復旧。

［目標復旧時点（RPO）］

・前日のバックアップ取得時まで復旧。

③ 重要業務のためのシステムの概要

a. 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 台あたり 100 名程度。サーバ利用状況は最も多いサーバで 500 万 PV/日。

b. 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、自社オフィスの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 4-95 に示す。

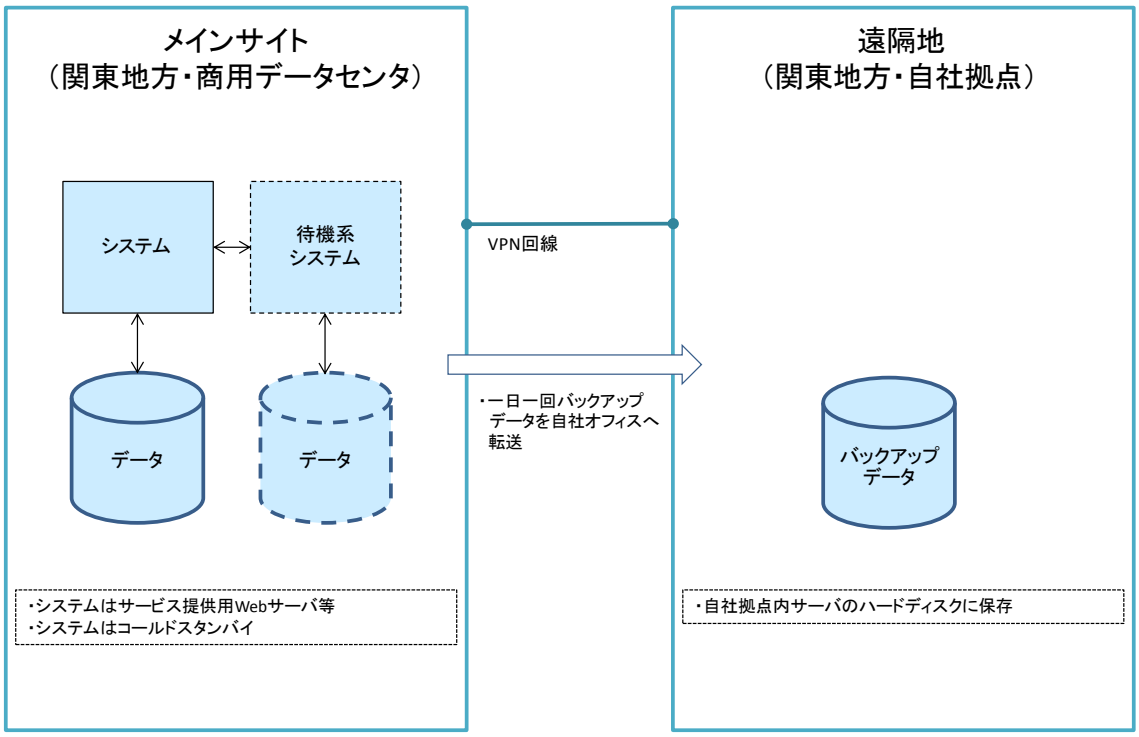


図 4-95 システム構成の概要

＜この構成を採用した理由や判断基準＞

・以前は、安定性とパフォーマンスを確保するため、サービス毎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。

・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。

c. 技術的特徴

＜ポイント＞

・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。

・ クラウドについて、ページヴュー数をカウントするためにIaaSを利用している。重要度もシステム負荷も低いため、手軽に使えるサービスであるため採用した。しかしながら、現時点ではクラウドサービスに重要なサーバをクラウドに移行するには、十分安定していないと感じている。実際、昨年は複数のクラウドサービスで長時間にわたりサービスを停止するようなトラブルが発生している。また、月額利用料については半年も利用すればサーバを購入できるような高価格であり、サーバを購入した方が低費用ですむと思われる。

④ システム復旧対策のポイントと留意点

a. 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。

b. ポイント

・ 費用を抑えながら、実施すべきと考える対策を実施した結果、現在の構成としている。(但し、担当者は相当のスキルが必要。)

c. 留意点や将来構想

・ 復旧の手順書については、さらに充実してゆきたい。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-11 のとおりである。

表 4-11 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		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
			RTO(目標復旧時間)	24 時間以内
			RLO(目標復旧レベル)	障害発生前と同等のレベル
		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)
	耐障害性	サーバ	冗長化(機器)	コールドスタンバイ
			冗長化(コンポーネント)	非冗長化
		ネットワーク機器	冗長化(機器)	非冗長化
			冗長化(コンポーネント)	非冗長化
		ネットワーク	回線の冗長化	非冗長化
			経路の冗長化	非冗長化
		ストレージ	冗長化(機器)	非冗長化
			冗長化(コンポーネント)	非冗長化
			冗長化(ディスク)	RAID1 による冗長化
		データ	バックアップ方式	オンラインバックアップ

大項目	中項目	小項目	指標	対策
			データインテグリティ	エラー検出無し
	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
		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
			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
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 ・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
			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。
	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
		予防保守レベル	予防保守レベル	予防保守を実施しない
	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
		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
			駆けつけ到着時間	定額保守契約は締結していない
			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）
		交換用部材の確保	保守部品確保レベル	確保しない
			予備機の有無	サーバ及びネットワーク機器に予備機あり
	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）
	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
		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
		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
		定期報告会	定期報告会実施頻度	実施していない
			報告内容のレベル	無し
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設されており、震度 7 相当まで耐えられる
		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

(4) D 社

① 企業の事業の特徴と IT

a. 業種・企業概要

・業種:金融・保険業

・業務内容:金融商品取引業務

・従業員数:約 850 名

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞

・システムにより提供するサービスそのものが業務であるため、システム依存度は非常に高く、経営層の関与度合いも高い。

＜IT 投資の比率＞

・IT 投資に係る費用(開発、運用、人件費、土地建物使用料、光熱費等を含む全費用)は、会社全費用の 1/3 程度を占めている。

＜IT の活用を促進する推進体制＞

・IT 関連業務は情報システム部門を構成する 3 つの部門(企画部門(企画計画を担当)、開発部門(開発・維持を担当)、サービス部門(運用・保守を担当))と品質管理部門が実施している。情報システム部門の統括を CIO が担っている。

・BCP の企画は企画部門で策定し、システムへの実装は開発部門で実施する体制である。IT 企画・検討および運用・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。

c. BCP の策定とマネジメント

＜策定時期と見直しの頻度＞

・策定時期は 2007 年、見直し頻度は年 1 回としている。

＜策定体制＞

・策定は、BCP 事務局にて実施する。BCP 事務局は BCP に関連する複数部門で構成されており、システム面だけでなく、ヒト、モノ、カネを含めた対応となっている。

・2006 年業界団体内で事業継続に係る検討 WG が開催され、業界として、「リスク事象の発現後おおむね 24 時間以内」を復旧・再開目標とし、全国の関係機関がそれに従って整備を進めている。

＜対象リスク＞

・事業におけるリスクとして、地震・風水害等の自然災害、システム障害、電力・通信等の社会インフラの停止、物理的破壊行為・サイバーテロ等のテロ行為、新型インフルエンザの流行等を想定し

ており、原因事象が発生することによりもたらされる結果事象としては、建物の利用不能、システムの利用不能、人員の不足、外部機関の停止等を想定している。

＜BCP 対応方針について＞

・ BCP は結果事象に基づいた対応方針を定めている。リスクが顕在化した際にも、必要な事業を継続するための体制・手順を規定している。対応方法は大きく 3 つに分かれており、センタの稼働状況により対応方法を定めている。

○1 点目は、「メインサイトの利用継続を前提とした対応」で、ケースとしては、大規模地震、風水害、テロ行為等により被害を受けているものの、メインサイトの利用は引き続き可能な場合を想定している。

○2 点目は、「バックアップサイトへの切替えを前提とした対応」で、ケースとしては、テロ、大規模火災等によりメインサイトが局所的に被害を受けている場合、または大規模地震等により、メインサイトおよび関連機関が同時に被害を受けており、バックアップサイトへの切替えが必要となる場合を想定している。

○3 点目は、「システム障害対応」で、取引を継続するよう努めること。ケースとしては、システムのハードウェアやアプリケーション障害、通信回線障害等により、システムが使用不能となった場合を想定している。

d. IT サービス継続計画（IT-BCP）の策定とマネジメント

＜IT-BCP の構成＞

・ 業務や IT 等を含む全体の BCP として策定しており、IT-BCP として策定は行っていない。

＜教育訓練や演習の実施と内容＞

・ 年間に何度か従業員向けの教育を実施（e ラーニング等含む）し、訓練も積極的に行っている。マニュアルも適宜改訂しながら訓練を継続実施しており、この訓練が有事の際の対応には有効と考えている。

e. 震災の影響

震災による直接被害は無くシステム面の見直しはとくに必要なしとの見解であり、運用面でこれまでの内容からいくつか見直しを行った。

○1 点目は、「事業継続に必要な人員確保が困難となる状況への対応」についてである。公共交通機関が使用不能となり、通常どおりの人員確保が困難な条件下であっても、事業継続が求められる業務を更に絞り込み、その遂行に必要な人員確保のための体制を整備した。併せて、有事の際に上記業務に従事する社員を対象に、公共交通機関を使用しない条件下での駆け付け訓練を実施した。

○2 点目は、「事業継続に必要な通信インフラが逼迫する状況への対応」についてである。災害時

に従業員および家族の安否を確認するためのツールである安否確認システムと緊急時連絡について運用を見直した。

○その他としては、備蓄品の見直し、事業継続基本計画書等マニュアルの見直しを行った。

② 企業の重要業務と継続戦略

a. 重要業務

＜選定した重要業務＞

・ 金融商品取引業務

b. 業務選定の理由・経緯

＜選定の理由や判断基準＞

・ 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。

＜戦略検討の方法＞

・ 復旧目標値については、業界全体で決められたルールであり、自社での設定では無い。

＜設定した目標＞

[目標復旧時間(RTO)]

・ 取引業務:24 時間以内復旧

[目標復旧レベル(RLO)]

・ 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)]

・ 障害発生直前まで復旧する。

③ 重要業務のためのシステムの概要

a. 規模

・ メインサイト:約 200 台

・ 取引処理件数　60 万件/分

b. 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 4-96 に示す。

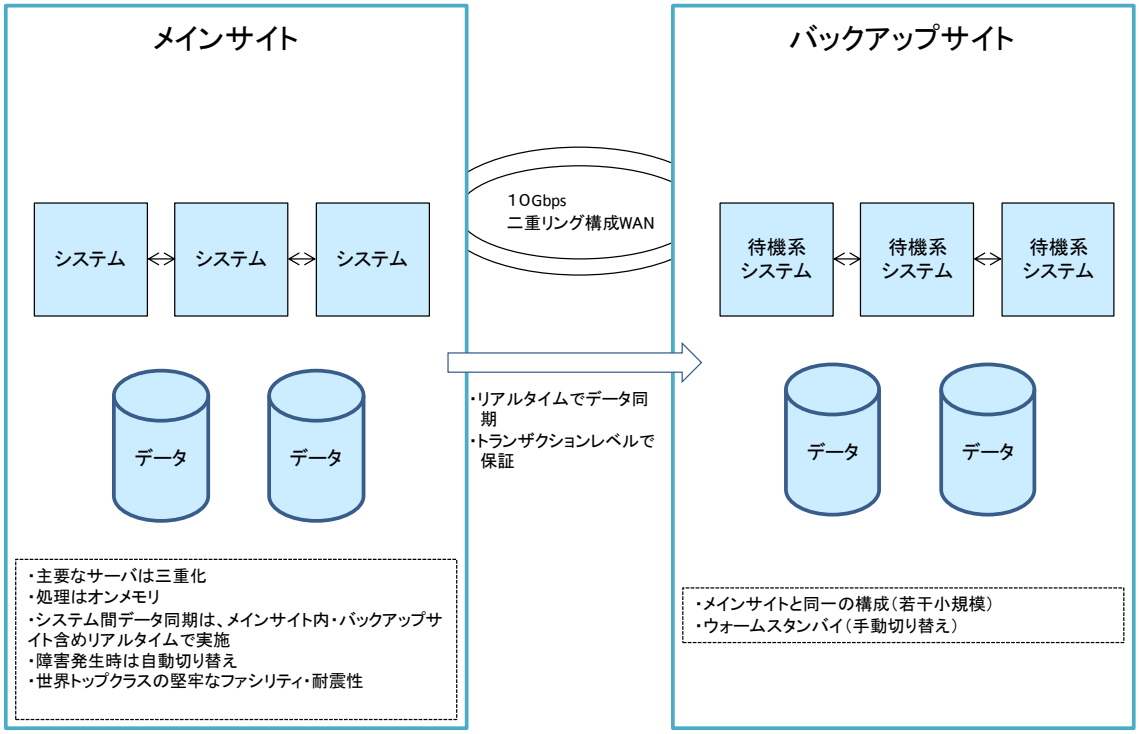


図 4-96 システム構成の概要

＜この構成を採用した理由や判断基準＞

・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。

・レスポンス重視のシステムであるためサーバ仮想化技術は当面導入予定が無い。

c. 技術的特徴

＜ポイント＞

・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としている。

・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。

④ システム復旧対策のポイントと留意点

a. 震災時等の効果

・直接の影響は無かった。

b. ポイント

・緊急時のマニュアルは、訓練を実施し、実行可能なマニュアルにしていくことが重要と考える。毎年シナリオを変え、訓練内容もステップアップしながら継続して実施している。その訓練に基づき、マニュアル等の改訂、体制の改善を図っている。

c. 留意点や将来構想

・首都直下地震を想定した対応の検討を今後行う。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-12 のとおりである。

表 4-12 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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）
		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）
			RTO（目標復旧時間）	ハードウェア故障時は停止時間 0 分
			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
		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
	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）
			冗長化（コンポーネント）	全てのコンポーネントを冗長化
		ネットワーク機器	冗長化（機器）	全ての機器を冗長化
			冗長化（コンポーネント）	全てのコンポーネントを冗長化
		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 か所のアクセスポイントに接続）
			経路の冗長化	全て冗長化
		ストレージ	冗長化（機器）	全て冗長化
			冗長化（コンポーネント）	全て冗長化
			冗長化（ディスク）	全て冗長化
		データ	バックアップ方式	オンラインバックアップ
			データインテグリティ	非回答
	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
		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
			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
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
			監視間隔	リアルタイム監視（最短は 1 秒間に数回）
	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）
		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
	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	・同一サイト内の切替えは自動化されている ・バックアップサイトは手動切替え
		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
			駆けつけ到着時間	保守員が 24 時間常駐
			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）

大項目	中項目	小項目	指標	対策
		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。
			予備機の有無	予備機は無い（三重化のため不要）
	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
	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（運用オペレータ）がセンタに常駐し一次対応を行う
		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
		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、構築委託先、ユーザも参加して訓練を実施している
		定期報告会	定期報告会実施頻度	月１回
			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
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
		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）

(5) E 団体

① 事業の特徴と IT

a. 業種・企業概要

・業種:地方公共団体(東日本大震災被災自治体)

・職員数:300 名弱

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞

・ 東日本大震災以前は、市全体のまちづくりの理念や施策を定める総合計画の分野別個別計画として情報化計画を定めており、この計画に基づいて IT を推進してきた。震災後の 1 年間は、震災前の IT 環境の復旧を目標としてきた。今後は長期的な情報化推進計画を策定する必要があるが、震災復興計画、庁舎や各公共施設の建設計画などがまだまだ不明確な現状にあり策定できていない。

＜IT の活用を促進する推進体制＞

・ 副市長が CIO を兼任している。副市長は、IT の専門家ではなく、IT の方針をトップダウンにより示すよりも、ボトムアップにより挙げられた計画を承認する立場である。

・ 全庁の情報化に関する業務を所掌しているのは情報システム部門であり、情報化計画策定、IT-BCP 策定、全庁的に関わるシステムや庁内基盤ネットワークの構築・運用管理等を担っている。なお、各部門個別で導入しているシステムは各部門個別に管理している。

＜IT の活用内容や効果＞

・ 自治体の窓口業務を始めとした各種の住民サービスを提供するにあたって、システムにより様々な情報を管理している。多くの住民サービスにおいてシステムを利用せずサービス提供することは考えられない。

・ 住民情報システムは、市民サービス提供と業務効率化に役に立っている。

・ 税務システムは、徴税管理と業務効率化に役に立っている。

c. BCP の策定とマネジメント

・ 市全体の BCP は未策定である。

d. IT サービス継続計画(IT-BCP)の策定とマネジメント

＜策定時期と見直しの頻度＞

・ 震災前にはIT-BCPを策定していたが、担当者が被災したことと、資料および電子ファイルが消失したことにより、内容については不明である。

・ 市全体のBCPと整合をとりながらIT-BCPについても検討してゆくことになると思うが、実施時期等

は未定である。

② 重要業務と継続戦略

a. 重要業務

＜選定した重要業務＞

・住民基本台帳システム
・税務システム
・財務会計システム
・人事管理システム
・メール・グループウェア
・公式ホームページ
・運用・セキュリティ関連システム

b. 業務選定の理由・経緯

＜検討の体制（経営層、業務担当課等の関与）＞

・システム復旧における業務選定に当たっては、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。

＜選定の理由や判断基準＞

・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。

c. 戦略の内容と検討方法

＜設定した目標＞

［目標復旧時間（RTO）］

・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。
・大規模災害時、最初の 3 日間自治体従業員は人命救助・安全確保に関する業務が最優先となる。システムの復旧にとりかかれるのは、それ以降となる。

［目標復旧レベル（RLO）］

・未設定
・システムの復旧優先順位としては設定している。例としては、住民の安否確認、り災証明発行等の要求から住民基本台帳システムを最優先とする等。

［目標復旧時点（RPO）］

・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。

③ 重要業務のためのシステムの概要

a. 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。

b. 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 4-97 に示す。

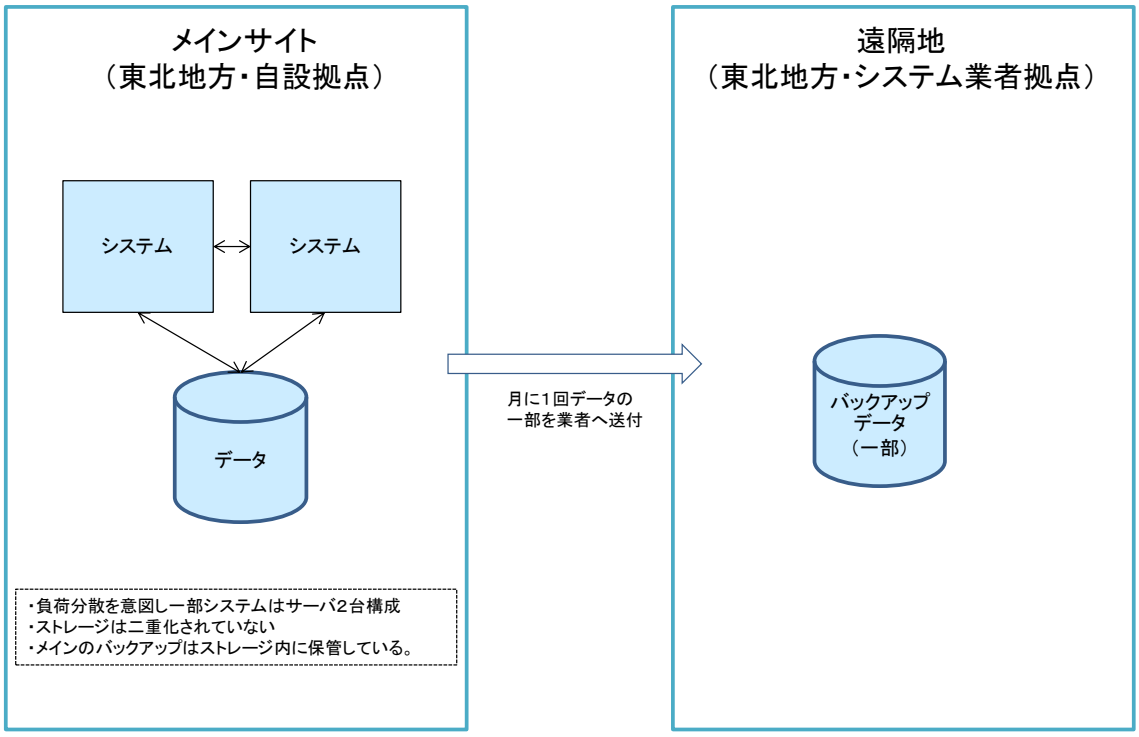


図 4-97 システム構成の概要

＜この構成を採用した理由や判断基準＞

・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従業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。）。

c. 技術的特徴

＜導入した技術・サービスの内容＞

・ブレードサーバを導入した。

・サーバとストレージは SAN で接続し、バックアップはストレージ内に保管する。

・委託先事業者によるシステム遠隔監視を充実した。

＜導入メリット＞

・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。

④ システム復旧対策のポイントと留意点

a. 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 はすべ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て復旧したりした。それでも、すべては復旧できず手作業で復旧しているものもある。

b. ポイント

・従業員だけでは技術的なスキルが不十分であり、物品調達や委託先事業者間の調整も非常に困難であったため、緊急的な措置として、住民基本台帳システムを納入していた委託先事業者に中心になってもらい、業者間調整等一部職員の業務に踏み込んだ形でシステム復旧作業に協力し

てもらった。

c. 留意点や将来構想

・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、従業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。

・震災を踏まえて、対策しておくべきと痛感した点は、以下の 4 点である。

○人の被災

今回の震災では当時のシステム担当者が被災した。そのためシステムの情報（システム構成、委託先事業者等）が分からず支障があった。これに対応するために、システムの情報をデータ化や書類化し、庁舎とは別の拠点に保管しておくべきであった。

○データの喪失

データが失われることは絶対に避けなければならず、対策は必須である。

○電気と通信の途絶

今回の震災では、電気と通信が途絶したことが復旧の大きな支障となった。通信環境に関しては、容量は少なくとも安定した通信環境を確保することが非常に重要である。有線ネットワークは敷設に時間がかかるため、被災直後には無線 LAN や衛星インターネット、特に衛星インターネットの活用が非常に有用であった。無線 LAN は学校給食センタと仮設の事務所間（約 150m）を接続する際に使用した。

○建物の喪失

今回の震災では、建物が津波被害で失われた。建物がなければ、対応作業を進めることはできない。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-13 のとおりである。

表 4-13 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		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）
			RTO（目標復旧時間）	数値としては定めていない
			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

大項目	中項目	小項目	指標	対策
		目標復旧水準（大規模災害時）	システム再開目標	数値としては定めていない
	耐障害性	サーバ	冗長化（機器）	一部冗長化している
			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
		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。
			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
		ネットワーク	回線の冗長化	非冗長化
			経路の冗長化	一部経路のみ冗長化されている
		ストレージ	冗長化（機器）	非冗長化
			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
			冗長化（ディスク）	RAID5 による冗長化
		データ	バックアップ方式	オンラインバックアップ
			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。
	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
		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
			保管方法	媒体による保管
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
			監視間隔	リアルタイム監視（分間隔）
	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）
		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
	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
		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
			駆けつけ到着時間	数時間内
			SE 到着平均時間	数時間内
		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
			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。
	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）
	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。
		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。
		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
		定期報告会	定期報告会実施頻度	実施していない
			報告内容のレベル	障害報告のみ
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
		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

(6) F 社

① 事業の特徴と IT

a. 業種・企業概要

・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

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞
・ 経営層自らが「お客様本意の活動」の心がけのもと、顧客へ質の高いサービスを提供するために従業員が安定かつ効果的にサービスを提供できるように全社に IT 化を積極的に推進している。
・ 売上高に対する投資率は、例年 1%程度である。
＜IT の活用を促進する推進体制＞
・ IT 企画・検討および運用・管理は情報システム部門が実施。施策は、専務(現 CIO)と社長(前 CIO)が意思決定している。
・ 情報システム部門は 2 名体制である。
＜IT の活用内容や効果＞
・ CTI 導入によって、お客様を特定することができ、購入履歴と売上を連動できるようになった。結果、顧客へのサービス向上にも役に立っている。
・ 勘定系のシステムは、業務効率化に役に立っている。
・ 販売管理システムは、販売促進と業務効率化に役に立っている。

c. BCP の策定とマネジメント

・ BCP は未策定である。

d. IT サービス継続計画(IT-BCP)の策定とマネジメント

＜策定時期と見直しの頻度＞
・ IT-BCP は未策定である。
・ 後述するように、水害被災経験があり、まずは対策を優先させた。後追いになるが今後、明文化を検討している。
＜策定体制＞
・ 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うこととなる。
・ 地元委託先事業者の支援を受けている。

＜対象リスク＞

・ 自然災害（その他、竜巻や高潮等）
・ インフルエンザや感染症等によるパンデミック
・ 建物や施設の破壊・損失
・ ハードウェアの故障
・ 停電

② 重要業務と継続戦略

a. 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）

b. 業務選定の理由・経緯

＜検討の体制＞

・ 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う。

＜選定の理由や判断基準＞

・ 重要業務の選定理由：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。

c. 戦略の内容と検討方法

［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）は未設定である（検討中）。
・ 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）は未設定である（検討中）。

③ 重要業務のためのシステムの概要

a. 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）

b. 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。

・通常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。

・システム構成の概要を図 4-98 に示す。

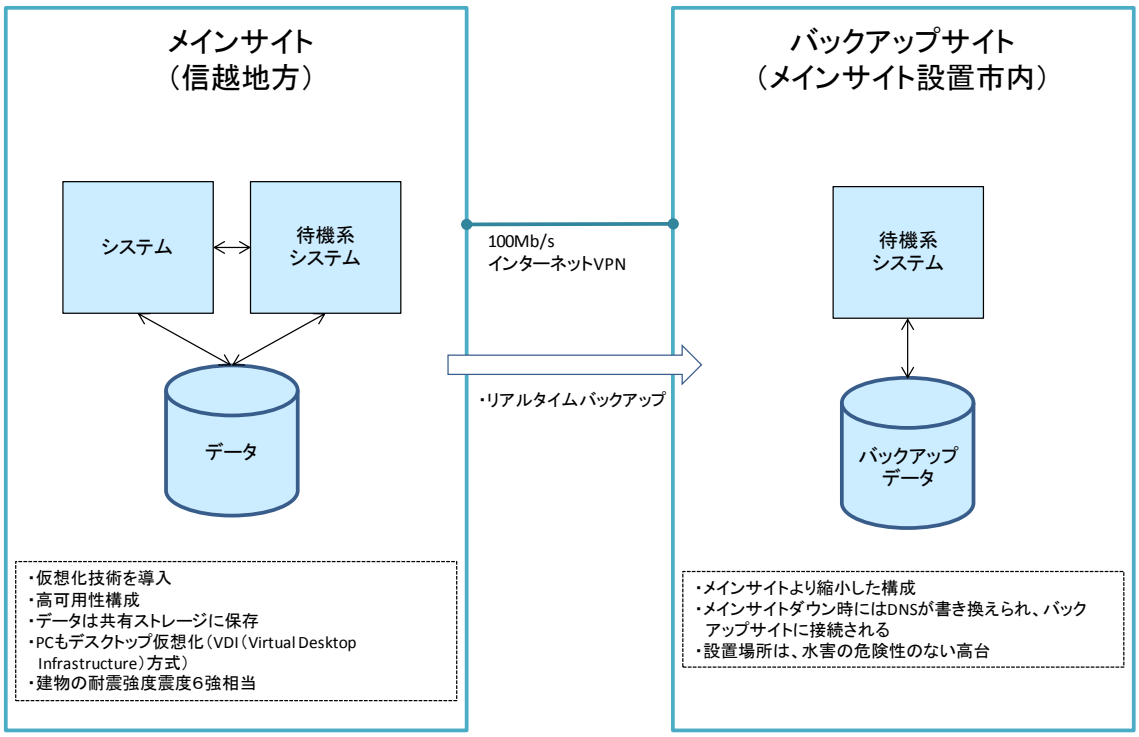


図 4-98 システム構成の概要

＜この構成を採用した理由や判断基準＞

・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、今回は、バックアップ環境構築の点のみで実施した訳ではなく、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。

・ 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。

＜対策の概算費用＞

・ 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。バックアップサイトのサーバを新規で構築した場合は、通常 500 万円程度追加となると想定される（データセンタ費用を除くハード・OS 費用のみ）。

・ 今回は、メインサーバ 2 台は、既存サーバを利用した。これを新規導入の場合のサーバ費用は、200 万円程度（1 台 100 万円程度×2 台）と想定される。

・ 仮に、仮想化を前提とした場合、ミラーサーバ構成の有・無でコストを比較すると、1.5:1 程度になると想定される。

c. 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）。

＜導入メリット＞

・ 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。

・ 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。

・ 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。

＜留意点＞

・ 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。

④ システム復旧対策のポイントと留意点

a. 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。

b. ポイント

・ 仮想化技術の採用は、先に示したように、非常にメリットが大きかった。

c. 留意点や将来構想

・ IT-BCP に関して、ネットワークの冗長化を検討している。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-14 のとおりである。

表 4-14 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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。
		目標復旧水準（業務停止時）	RPO（目標復旧時点）	障害発生時点
			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
			RLO（目標復旧レベル）	・特定の業務 ・性能は低い水準を許容
		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
	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
			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
		ネットワーク機器	冗長化（機器）	非冗長化
			冗長化（コンポーネント）	非冗長化
		ネットワーク	回線の冗長化	非冗長化
			経路の冗長化	非冗長化
		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）
			冗長化（コンポーネント）	電源・FAN は冗長化している
			冗長化（ディスク）	RAID5 以上
		データ	バックアップ方式	オンラインバックアップ
			データインテグリティ	エラー検出及び再試行を実施
	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
		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
			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
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
			監視間隔	リアルタイム監視（秒間隔）
	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
		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

大項目	中項目	小項目	指標	対策
	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	・バックアップサイトへの切替えは自動化（自動で DNS の切替え実施） ・クライアント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は通常の PC として動作させることも可能
		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
			駆けつけ到着時間	数時間内
			SE 到着平均時間	数時間内
		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
			予備機の有無	・ネットワーク機器、クライアントは予備機有り ・サーバはリプレース前のものを予備機としている
	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
	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
		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
		オペレーション訓練	オペレーション訓練範囲	サーバ切替えの訓練は実施していない（導入時にテストを実施）
		定期報告会	定期報告会実施頻度	実施していない
			報告内容のレベル	無し
システム環境	機材設置環境条件	耐震/免震	耐震震度	建設は 1981 年以降なので、震度 6 強にも耐えられる
		電気設備適合性	停電対策	自家発電装置により、40 時間程度電源を確保することができる

(7) G 社

① 事業の特徴と IT

a. 業種・企業概要

・業種:機械製造業

・従業員数:約 300 名

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞

・業務全般における情報管理を目的とし IT を活用している。具体的には受発注管理、入出荷管理、原価管理、作業工数管理等の業務である。経営の意思決定をサポートするところまでは達していないが、経営層等への各種報告に利用する基礎データをシステムで管理している。

＜IT の活用を促進する推進体制＞

・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。IT 運営委員会は経営層 6 名と情報システム部門の責任者により構成され、委員長は専務である。情報システム部門の従業員は 5 名である。

＜IT 投資の比率＞

・社全体の年間売上は 40 億円程度であるが、そのうち年間 IT 投資は 2 千万円程度である。IT 投資は主にソフトウェアに係わる費用が多く占める。

＜震災による変化等＞

・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。

c. BCP の策定とマネジメント

＜BCP 対応方針について＞

・社全体の BCP については東日本大震災を機に経営層を中心に検討を開始したと聞いているが、未完成ということもあり社全体への内容の周知は実施されていない。

d. IT サービス継続計画(IT-BCP)の策定とマネジメント

＜BCP と IT-BCP の連携状況＞

・IT-BCP は IT 運営委員会を中心に検討しているが、BCP が社内周知されていないので、連携はしていない。会社全体の BCP よりも IT-BCP の方が検討はすすんでいる。

・システムが停止しても業務が完全に停止するわけではないので、社としてはなるべく IT に費用をかけない方針である。一方、内部統制監査を依頼している公認会計士からは IT に関する改善の

指摘が多く、指摘のあった事項は対応することが多い。

＜教育訓練や演習の実施と内容＞

・システムの保守に関しては委託先事業者にすべて任せているので、従業員は大規模災害時のシステム復旧に関する特別な教育・訓練を受講していない。システム操作に関する研修は、受講している。

② 重要業務と継続戦略

a. 重要業務

＜選定した重要業務＞

・生産管理システム

b. 業務選定の理由・経緯

＜選定の理由や判断基準＞

・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。なお、将来的に経理課の原価計算システムは統合する予定である。

＜戦略検討の方法＞

・2 週間程度のシステム停止であれば、その間は紙等を使用した代替手段を用いることで業務を継続できると考えている。

・サーバハードウェア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。

＜設定した目標＞

[目標復旧時間(RTO)]

・大規模災害時:2 週間程度

[目標復旧レベル(RLO)]

・対象システムは生産管理、財務、経理システムの 3 つすべてである。

・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)]

・障害発生前日のバックアップ時点まで復旧する。

③ 重要業務のためのシステムの概要

a. 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。

b. 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 4-99 に示す。

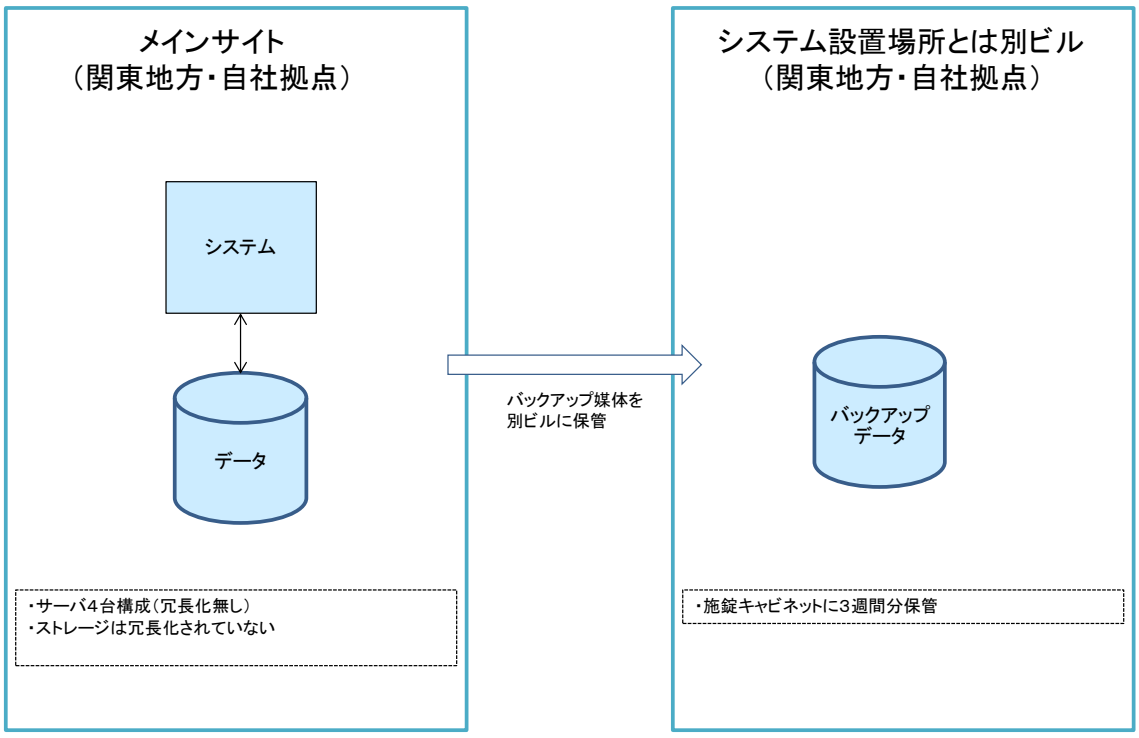


図 4-99 システム構成の概要

＜この構成を採用した理由や判断基準＞

・バックアップ媒体をサーバ設置場所とは別なビルの施錠キャビネット内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。

c. 技術的特徴

＜ポイント＞

・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。

④ システム復旧対策のポイントと留意点

a. 震災時等の効果

・ 直接の影響は無かった。

b. ポイント

・ 経営層は IT 投資にはあまり意欲的ではないが、公認会計士の指摘により、バックアップ保管場所の変更、建物の耐震対策見直し等を実施した。

c. 留意点や将来構想

・ バックアップデータはデータ数の一致を年に一度確認しているが、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。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-15 のとおりである。

表 4-15 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		目標復旧水準（業務停止時）	RPO（目標復旧地点）	日次バックアップからの復旧
			RTO（目標復旧時間）	半日程度
			RLO（目標復旧レベル）	全ての業務
		目標復旧水準（大規模災害時）	システム再開目標	2 週間
	耐障害性	サーバ	冗長化（機器）	非冗長化
			冗長化（コンポーネント）	非冗長化
		ネットワーク機器	冗長化（機器）	非冗長化
			冗長化（コンポーネント）	非冗長化
		ネットワーク	回線の冗長化	非冗長化
			経路の冗長化	非冗長化
		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
			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
			冗長化（ディスク）	内蔵ハードディスクについて RAID5
		データ	バックアップ方式	オンラインバックアップ
			データインテグリティ	非回答
	災害対策	システム	復旧方針	代替機による同等の構成
		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
			保管方法	媒体による保管
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
			監視間隔	リアルタイム監視（分間隔）
	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
		予防保守レベル	予防保守レベル	予防保守を実施しない

大項目	中項目	小項目	指標	対策
	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
		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
			駆けつけ到着時間	数時間内
			SE 到着平均時間	数時間内
		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
			予備機の有無	予備機無し
	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）
	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
		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
		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
		定期報告会	定期報告会実施頻度	実施していない
			報告内容のレベル	障害報告のみ
システム環境	機材設置環境条件	耐震/免震	耐震震度	建設は 2 年前なので震度 6 強に耐えられる
		電気設備適合性	停電対策	UPS により、10 分程度の電源を確保することができる

(8) H 社

① 事業の特徴と IT

a. 業種・企業概要

・ 業種:サービス業
・ 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

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞
・ 現在、経営理念や経営戦略においても IT の活用方針や位置付けは示されていないが、今後策定予定の中長期計画では示していきたいと考えている。
・ ＜IT を活用して得られた効果＞
・ IT は当社の本業そのものを支えるものであり、事業を成立させている根幹である。
・ なお、業務としては受託開発が大半であるが、年間数百の受託案件うち 5 つ程度、ユーザ数の少ない特定顧客向け ASP サービスの提供も実施している。
＜IT の活用を促進する推進体制の有無＞
・ 情報システム部門は、全社的なネットワークなどの基盤部分を担当している。顧客システムの開発環境となるサーバ等の機器等は各部門が購入・管理している(部門採算性)。
・ IT-BCP は全社 BCP の一環として人事総務部が作成している(IT-BCP のみの単独作成は行っていない)。バックアップなど災害に向けた事前対策は情報システム部門が行っているため、IT に関する BCP を策定する組織と実装する組織は同一と言える。
・ ただし、実際に災害が発生した時に、情報システム部門だけで対応することは困難と予想されるため、各部門にも役割を持たせることが必要だと考えている。

c. BCP の策定とマネジメント

＜策定時期と見直しの頻度＞
・ 現行の BCP(ver.1)は 3 年前に策定した。社会的に問題意識が高くなっていたことが、策定の契機となった。
＜対象リスク＞
・ 対象としているリスクは地震であり、首都圏直下型震度 6 弱を想定している。
・ 定期的な見直しを行うことは定めていないが、内容充実に向けて見直しを図りたいと考えている。
＜策定体制＞
・ COO からも見直しの指示が出ており、新たな BCP は COO をトップに策定する予定である。ビジ

ネスインパクト分析（BIA）や目標復旧時間（RTO）の設定には、投資も関係するため、そこも含め経営層の判断を仰ぎたい。素案は情報システム部門が作成する予定である。

d. IT サービス継続計画（IT-BCP）の策定とマネジメント

＜策定時期と見直しの頻度＞

・IT-BCP として独立した文書は作成していない。今後も BCP と一体的なものとして策定する。

＜計画の構成＞

・BCPver1 において、IT 関連事項としては対策実施計画（遠隔地でのバックアップ対策）、緊急時対応計画（緊急時の安否確認方法、対策本部の設立方法）を定めている。全体的に、入口部分（基本的な考え）は決めているものの、具体的な内容が示されておらず、実効性があまり高くないと考えられる。

・社としての重要業務はあまり明確に定義されておらず、目標復旧時間も定めていなかった。分析に要する知識やノウハウが社内になかったため、ビジネスインパクト分析（BIA）も行わなかった。また、教育訓練計画についても定めていない。

・現在は、社内に BCP 策定のコンサルティング業務を顧客から請け負っている部門があるため、ここでのノウハウを活用して見直しを図りたいと考えている。

＜BCP と IT-BCP の関係＞

・ver1 と同様、今後も IT-BCP は全社 BCP の一環として作成する予定である。

＜震災の影響＞

・震災によって特段の影響はなく、以前より BCP の充実が必要だとの認識はあったため見直しを図ることになった。

② 重要業務と継続戦略

a. 重要業務

＜事業の IT 依存度＞

・IT 自体が商品であり、IT への依存度は非常に大きい。

・社員と連絡が取れないと顧客対応が不可能となる。また、これまで開発したシステムや開発中のシステムの損失は、事業を行う上で大きな被害につながる。

＜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すべて同じレベルで「重要」と位置付けられており、すべ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。次に開発しているソフトウェアである。

・各部門が保有する顧客用のシステム・データについては、バックアップサーバの容量割当内に収まる範囲で、各部門がバックアップ対象を決めてきた。ただ、顧客データのバックアップ対象選定ルールが明確になっておらず、選定は部門判断となっているため、重要な顧客のシステムやデータが確実にバックアップされているか分からないといった問題を抱えている。全社的には機密情報、重要度といった一定の指標を情報セキュリティ規程において定めているが、実際に各部門のバックアップ対象選定に判断基準に活用できるほどの具体性はない。

b. 業務選定の理由・経緯

・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。

c. 戦略の内容と検討方法

・ビジネスインパクト分析（BIA）を行っておらず、全社的な戦略の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

③ 重要業務のためのシステムの概要

a. 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。

b. 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。

・また、遠隔地に待機系システムがあるシステムとしては、財務会計管理システムがある。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 4-100 に示す。

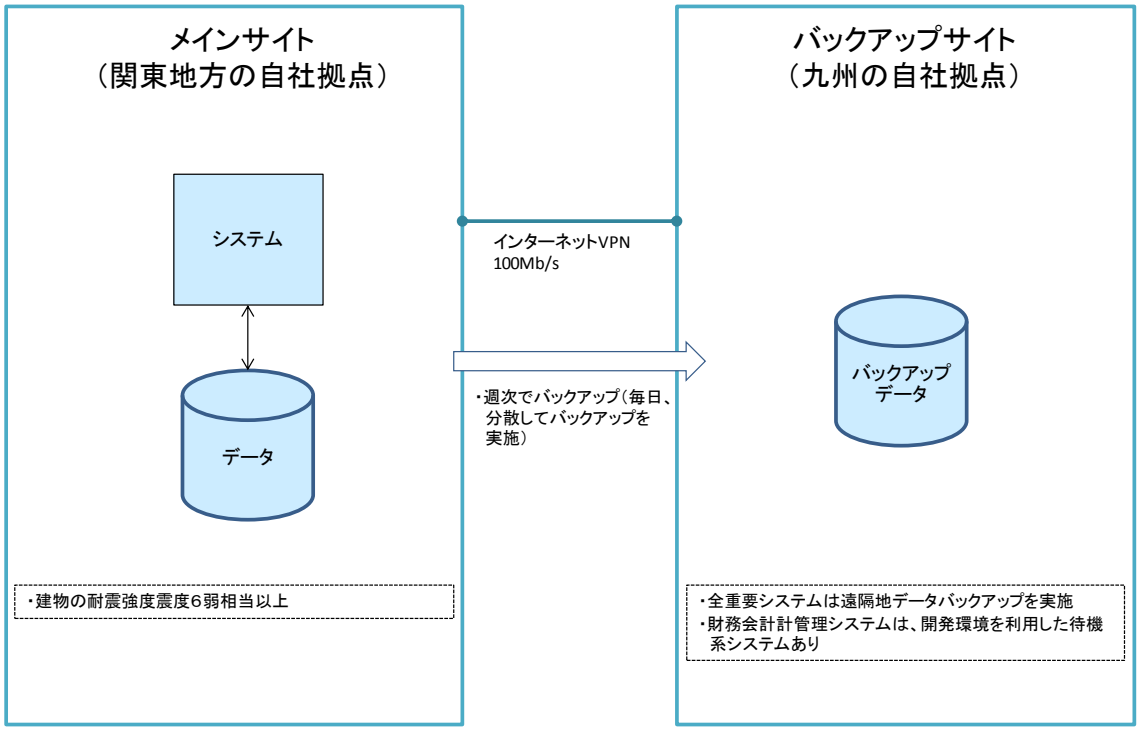


図 4-100 システム構成の概要

＜この構成を採用した理由や判断基準＞

・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。

・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。

・財務会計管理システム、メール・グループウェアシステムのサーバの二重化については、他システムと吟味した上でこれらを選定したわけではないが、これらは即時の復旧が必要であり、構築予定額内で実現可能だったため二重化した。

・財務会計管理システムの待機システムを置いた理由は、一部は自社開発であり、開発時に使用したデモ機器が遠隔地におかれているため、これを待機系システムとして位置づけていることにある。データをバックアップサイトから移せば使用可能であるが、自動切り替えはできないところが問題である。

c. 技術的特徴

・顧客用システム用の一部ファイルサーバについて仮想化しているものもある。

・顧客用システムの開発の際、複数の OS バージョンの開発環境を構築するのに、仮想化は有効だった。

・一方で、仮想化のためにシステムによっては動作速度が遅いといった弊害も見受けられる。

④ システム復旧対策のポイントと留意点

a. 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。

b. ポイント

・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求められる。

c. 留意点や将来構想

・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。

＜クラウドの利用＞

・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。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-16 のとおりである。

表 4-16 システム復旧対策の詳細

大項目	中項目	小項目	指標	調査特記
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
		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。
			RTO（目標復旧時間）	未設定。10～30 分未満を目指したい。
			RLO（目標復旧レベル）	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。
		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
	耐障害性	サーバ	冗長化（機器）	一部冗長化している
			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
		ネットワーク機器	冗長化（機器）	非冗長化
			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
		ネットワーク	回線の冗長化	非冗長化
			経路の冗長化	非冗長化
		ストレージ	冗長化（機器）	特定の機器のみ冗長化
			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
			冗長化（ディスク）	RAID5 による冗長化
		データ	バックアップ方式	オンラインバックアップ
			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）
	災害対策	システム	復旧方針	未対策
		外部保管データ	保管場所分散度	1 ヵ所(遠隔地)
			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
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
			監視間隔	リアルタイム監視（分間隔）
	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
		予防保守レベル	予防保守レベル	予防保守を実施しない
	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
		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）
			駆けつけ到着時間	センドバック保守。電話対応は随時。
			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。
		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
			予備機の有無	ネットワーク機器については予備機あり
	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
	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
		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

大項目	中項目	小項目	指標	調査特記
		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
		定期報告会	定期報告会実施頻度	実施していない
			報告内容のレベル	無し
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
		電気設備適合性	停電対策	UPS により、1 時間分程度の電源を確保することができる

(9) I 社

① 事業の特徴と IT

a. 業種・企業概要

・ 業種:サービス業
・ 空間情報コンサルティングを主要事業とするサービス業の持株会社。
・ 従業員数:約 2,000 名(グループ連結)
・ 事業拠点:約 50 拠点(グループ連結/国内・海外拠点含む)

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞
・ 持株会社で決定した経営方針のもとに、この 3 年間でシステムの更改を図ってきた。
・ グループ全体の事業運営を行う上で、大きく以下の 3 つに分類される業務がある。このうち持株会社では、1)、2)をマネジメントしている。
1)グループ企業全体の基幹業務
○グループの基幹業務となる ERP システム
○持株会社が管理・運用
2)グループ企業全体のメール・グループウェアシステム(Web サイトを含む)
○事業運営に必要不可欠なメールとグループウェアシステム
○持株会社が管理・運用
3)各事業会社が保有するシステム(社外向けの事業(サービス)含む)
○各事業会社が商品・サービス提供を行うための個別システム
○各事業会社が管理・運営

＜IT 投資の比率＞
・ 更改前の年間費用は約 3 億円であり、売上額の 0.6%程度の比率である。
・ 震災以前の当初計画では年間費用の 3 割から 4 割削減し、年間費用 2 億円を目標にしていた。東日本大震災や計画停電等の影響を受けた経験を踏まえた対策に投資額が増加し、結果的に昨年度の年間費用は約 5 億円となったが、同じ年間費用で対策を実施し、事業継続性を向上させる結果となった(開発に約 2 億円、運用費用約 3 億円)。

＜IT を活用して得られた効果＞
・ グループウェアや ERP システム導入後の 10 年間の経過をみると、「経営の見える化」、「業務効率化」の面で効果が得られた。
・ 特に、全国の生産拠点、営業拠点と海外拠点を有する事業体制においては、営業担当と技術者とのコミュニケーションツール、基幹系業務として不可欠で重要なシステムとなっている。

＜IT の活用を促進する推進体制の有無＞
・ 計画策定は、持株会社で機関決定される。

・BCP の策定は、リスク管理委員会（委員長は社長、リスク担当役員：各事業者役員）にて、最終決定を実施した。
・BCP は、安否確認等、IT 分野だけでなく人事部門や総務部門等、横断的に関わるため、計画の統括は総務部にて実施する。
・IT に関する内容は情報システム部門にて企画・管理・運用を実施する。
・BCP と IT-BCP は一体化したものとして取り組んでいる。

c. BCP の策定とマネジメント

・BCP は策定中である。IT-BCP を包含するものである。

d. IT サービス継続計画（IT-BCP）の策定とマネジメント

＜策定時期と見直しの頻度＞
・外部のコンサルティング支援を受けて検討し、素案を策定した段階である。
・震災後は対策の実施を優先する必要があった。計画は追って策定している。
・BCP 計画の見直しは、中期計画と連動するため、毎年、リスク管理委員会に事業計画とあわせてローリング方式で見直しをすることとなっている。東日本大震災のように、今後大きな災害が発生した際には随時見直しを行う。今年度は、関西圏の計画停電の影響が考えられる。
＜策定体制＞
・持株会社経営層や各事業会社幹部で構成されるリスク管理委員会により検討している。
・情報システム部門は、対策を実現する過程の中で関与した。
＜対象リスク＞
・地震・津波等による建物や施設の破壊・損失
・大規模災害に起因した停電（計画停電）
＜震災の影響＞
・リスク管理委員会は以前より運営しており、BCP 対策の検討も実施していた。例えば、海外拠点におけるテロ対策やインフルエンザ等のパンデミック対策、その他盗難等はリスクとして対策を講じていた。これらの対策により、東日本大震災は乗り切ったが、新たに地震や津波といった大規模災害に起因する停電等のリスクが明確となり、重点的に取り組む契機となり、東日本大震災以降具体的な対策が加速した。

② 重要業務と継続戦略

a. 重要業務

＜事業の IT 依存度＞
・IT が利用できない場合には、停止する業務もあり、IT の依存度は高い。
・当社の主要業務である、各グループ会社の事業統括の業務が不可能になる。

・グループ会社の拠点は全国各地に分かれており、IT を利用しない限り業務遂行は不可能である。

＜重要業務＞

・ERP システム（管理会計・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

b. 業務選定の理由・経緯

＜選定の理由や判断基準＞

・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。

＜検討の体制（経営層、業務担当課等の関与）＞

・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。

・事業会社の個別システムは各事業会社にて管理・運用している。

c. 戦略の内容と検討方法

＜目標復旧時間（RTO）等の目標設定のための方法＞

・震災を受け経営層からは、遠隔地に待機系システムを構築し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検討して決められた。

・内部向けの基幹系業務システム（ERP システム）と外部向けのメール・グループウェアシステムの 2 つについて、対応の優先度を重要視し検討した。

［ERP システム］

・ERP システムの復旧目標について、経営層は同期バックアップを実施し、待機系システムへの瞬時切り替えが必要性と考えていたが、この方式は約 1.5 億から 2 億程度の投資が必要であるため、業務の実態やコストを踏まえて、様々な実現パターンを検討した。

・検討の結果、同期バックアップを実施する場合に比べ、費用が半分または 1/3 程度に収まる一日 1 回のバックアップとする方式を選定した。サーバは関東・近畿のデータセンタ 2 か所に同じ環境を構築し、夜間の遠隔バックアップによって少なくとも 1 日前のデータに復旧可能とした

［メール・グループウェア等（外部向け Web サイト含む）］

・外向けの Web サイトは、瞬時に情報提供を行うことが必要不可欠であり、情報の送受信や意思決定のツールとしてメールやグループウェアも同様にサービスを継続する必要がある。

・特に震災時等は、災害時の写真等の画像を送受信する業務があり、内部向けの基幹系システムとは別に基準を設けて対策を実施している。

・

＜検討の体制（経営層、業務担当課等の関与）＞

・情報システム部門によって企画検討を実施し、経営会議にて最終承認を得て決定した。

＜設定した目標（ERP システム）＞

［目標復旧時間（RTO）］

・1 日～3 日未満

［目標復旧レベル（RLO）］

・障害・被災前と同等の業務を実施できる水準

［目標復旧時点（RPO）］

・障害・被災発生の前日まで復旧

＜理想の水準と実装した水準の差異＞

・経営層は、より短い目標復旧時間（RTO）を望んだが、費用対効果を考え、現在の目標となっている。

③ 重要業務のためのシステムの概要

a. 規模

［ERP システム］

・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（臨時雇用者含む）

b. システム構成と復旧対策の概要

［ERP システム］

・メインサイトとバックアップサイト同一構成であり、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。

・ネットワークは、メインサイトとバックアップサイト間はデータセンタ業者の提供するネットワークサービス（100Mbps：帯域保証）で接続し、ループ構成であり冗長化を確保している。

・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。

・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 4-101 に示す。

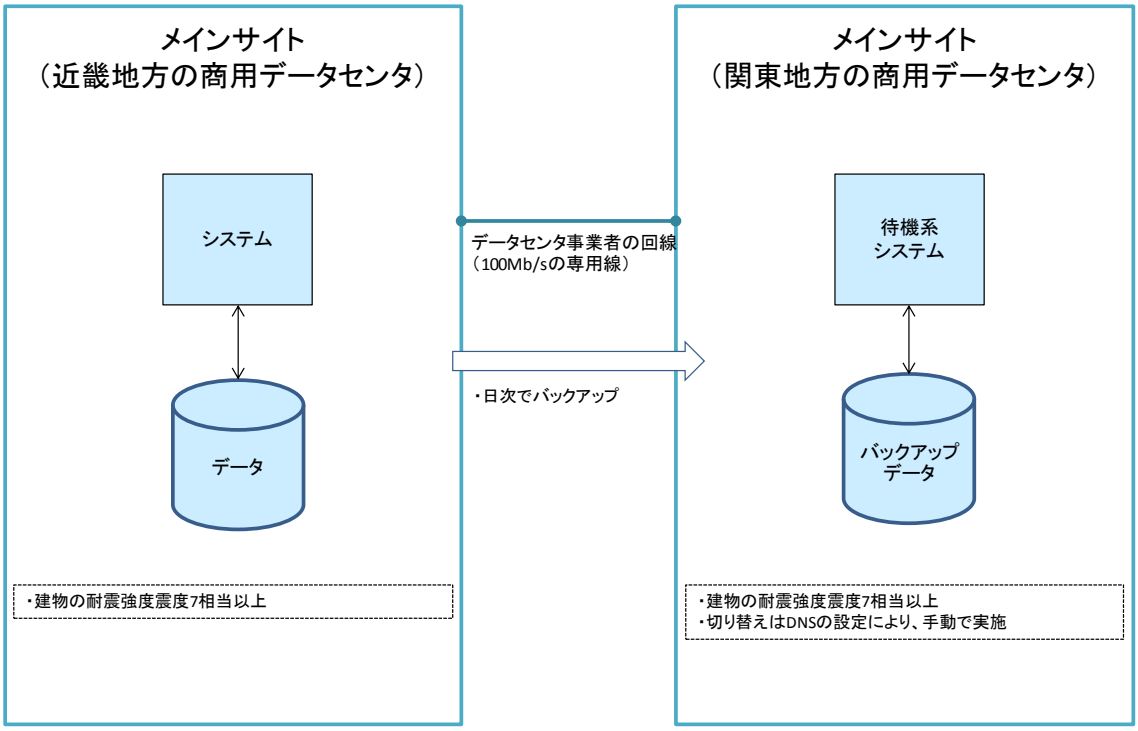


図 4-101 システム構成の概要

[メール・グループウェア等(外部向け Web サイト含む)]

・クラウドサービスを利用している。

・通常の利用時には、社の認証基盤により認証して利用するが、非常時には、認証基盤の認証なしに、インターネットからアクセスして利用できるようにし、サービスの継続性を確保する予定である。

＜この構成を採用した理由や判断基準＞

[ERP システム]

・3 つの実現パターンを比較検討した。パターンは、委託先事業者の助言をベースに情報システム部門で精査した。

・3 つの実現パターンと概算費用は以下のとおりである。

パターン①:同期バックアップ(ホットスタンバイ):約 1.5 億円

パターン②:夜間バックアップ(ウォームスタンバイ):約 5,000 万円

パターン③:遠隔地バックアップ:約 1,500 万円

・協議を重ねた結果、業務継続にはバックアップデータだけでなく、演算処理・検証するプログラムがなければ実現は難しくパターン③では不足、パターン①は投資額が大きいことから、パターン②とする、という結論に至った。
・ERP システムを更改する際に、監査法人からは IT 統制に対応可能なアウトプットを出力可能な情報システムであることが求められた。特に会計情報はバックアップデータからの再計算によって同じアウトプットを再現することが難しく、実施にあたって多大な労力も必要となる。また、ERP システムは 7 つのサブシステムが稼働しており、処理方法が統一されておらず復旧手順も統一できない状態であった。アプリケーション、ハードウェア構成等も、統一されていなかったため、データバックアップのみでは復旧が困難であること、復旧できたとしても時間を要することから、バックアップサイトにも待機系システムを設置する構成とした。

［メール・グループウェア等（外部向け Web サイト含む）］
・クラウドサービスを利用することが、業務停止しないために最適と考えた。
・メールは、世界中どこからでもアクセス可能であること、世界にサーバが分散されていることから、グローバルに展開するメールサービスを採用した。
・それまで使用していたポップサーバが老朽化していたこともあり、以前からクラウド利用を検討していた経緯もある。

c. 技術的特徴

＜導入した技術・サービスの内容＞
・プライベートクラウド（ERP システム以外は、データセンタに設置したサーバ仮想化環境へ移行した。）
・パブリッククラウドサービス（メール・ポータル、認証基盤）
・閉域網接続（VPN）

＜クラウド導入のメリット＞
・事業継続性が確保された。
・運用負荷が軽減された。
・事業継続性確保等のメリットが増えたがさほどコストを上げずにすんだ。支出費用はデータセンタ使用料等があるため単純に安くはならない。必要とするハードウェアリソースの予測が困難な場合は自社でハードウェアを保有せず、柔軟にリソースを増減可能なクラウドサービスを利用することが望ましいと考えている。

＜想定していたクラウド導入メリットに対するギャップ＞
・一部のクラウドサービスは安いものもあるが、すべてのサービスが安いとはいえない。
・投資金額だけを見ると、自前でサーバを購入した方が安い。ただし、場所・設備・機器・運用人員等のトータルコストでみると、安くなっていると考えている。また、部分的にアウトソースするよりもある程度まとめてアウトソースした方がコストメリットを得られると考えている。

＜クラウド利用上の留意点＞

・当初、関東地方のデータセンタとIaaSのクラウド環境に2台のDNSサーバを運用していたが、関東地方のデータセンタに接続する回線がダウンした場合 DNS サーバがまったく利用できなくなるため、近畿地方のデータセンタにDNSサーバを追加した。

・災害対策として、拠点間 LAN（インターネット VPN）の構成が関東地方のデータセンタを中心としたスター型となっていたが、近畿地方のデータセンタからの2拠点を中心としたスター型に変更した。

・クラウドサービスは、提供者の都合によってバージョンアップが行われるため、いつのまにか画面が変更になっていることもあり、エンドユーザから質問されることがある。ただし、業務への影響はない。

・セキュリティ面で工夫した点は、社内ネットワークとクラウドサービスとの接続ポイントを一元化して管理し、リスクを軽減している点である。

・海外では、プロトコルによりアクセス制御がかかる国もある（以前利用していた、IPSECは海外の国ではアクセス制御がかかってしまう時もあったが、SSL-VPN を利用することでこの問題をクリアした）。

＜今後導入や利用拡大を検討しているサービス＞

・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、今後はすべてを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。

④ システム復旧対策のポイントと留意点

a. 震災時等の効果

・現システムは、東日本大震災後の約3か月間で構築したシステムであるため未検証である。

b. ポイント

＜構築時に工夫した点・成功した点＞

・大規模災害や停電等の対応のため、サイトを分散させたことが工夫点である。

・従前のシステムは、計画停電等、停電が長期化する可能性のある中で、発電のための燃料確保に苦労した。2006 年に起きた大規模停電をうけて自家用発電機を導入したが、当時は 1 日以上の停電は無いと想定していたので、危険物取扱責任者が在籍しなくても対応できる重油量備蓄量は 30 時間であり、それで十分対応できると考えた。しかし、計画停電の際は、重油を追加しなければならなかった。現在も重油自体を自社でも貯蓄している。

c. 留意点や将来構想

・停電時はクライアント端末が利用できないこと、ネットワーク障害が発生する可能性があり継続性に懸念があるため、検討・対策を推進する。

⑤ システム復旧対策の詳細

システムの復旧対策の詳細は、表 4-17 のとおりである。

表 4-17 システム復旧対策の詳細(断りがない限り ERP システムについて記載)

大項目	中項目	小項目	指標	対策
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
		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
			RTO(目標復旧時間)	数時間以内
			RLO(目標復旧レベル)	ERP の全ての業務
		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
	耐障害性	サーバ	冗長化(機器)	全てのサーバで冗長化
			冗長化(コンポーネント)	全てのコンポーネントを冗長化
		ネットワーク機器	冗長化(機器)	全ての機器を冗長化
			冗長化(コンポーネント)	全てのコンポーネントを冗長化
		ネットワーク	回線の冗長化	データセンター本社間を冗長化
			経路の冗長化	一部冗長化
		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)
			冗長化(コンポーネント)	一部冗長化
			冗長化(ディスク)	RAID5 以上による冗長化
		データ	バックアップ方式	オフラインバックアップ
			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)
	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
		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
			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
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
			監視間隔	リアルタイム監視(分間隔)
	保守運用	定期保守頻度	定期保守頻度	年 1 回
		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
	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
		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
			駆けつけ到着時間	データセンタ内に保守要員が常駐
			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
		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
			予備機の有無	予備機無し
	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
	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
		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
		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
		定期報告会	定期報告会実施頻度	月 1 回

大項目	中項目	小項目	指標	対策
			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
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
		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

(10) J 社

① 事業の特徴と IT

a. 業種・企業概要

・業界各社が扱うサービスの普及啓発事業、品質の向上に関する事業、教育研修に関する事業に加え、組織加盟各社が共同で利用するシステムの構築や運用を行う業界団体である。
・従業員数:約 300 名

b. 全社レベルの IT ガバナンス

＜経営戦略と IT 活用の関係＞
・事業を遂行するにあたり、必ずしも IT は必要ではないが、業務効率面から考慮すると欠かせないものとなっている。
＜IT 投資の比率＞
・IT 関連費用は年間 5 億円程度である。
・費用は、システム利用各社が負担している。
＜IT の活用を促進する推進体制＞
・組織内部の情報システムは総務部門が担当し、組織に加盟する各社が利用するシステムは、当組織のシステム関連部門が構築から運用まで担当している。
・当組織のシステム関連部門の要員は 10 名程度である。

c. BCP の策定とマネジメント

＜策定時期と見直しの頻度＞
・2000 年頃に策定し、非定期に見直している。最近では 2009 年に見直した。現在、東日本大震災を機に見直しを進めているところである。
＜BCP 策定体制＞
・組織内に設置されている委員会において BCP の検討を進めている。委員会は組織加盟各社が構成員となっている。
＜BCP 対応方針について＞
・地震やインフルエンザ等によるパンデミック等の個別のリスクを想定した対応方針が策定されており、総合的な BCP 対応方針とすべく、現在見直し中である。

d. IT サービス継続計画(IT-BCP)の策定とマネジメント

＜策定時期と見直しの頻度＞
・一部のシステムを対象とした IT サービス継続に係る計画を策定している。IT サービスの中断や停止に備えた事前対策(代替システムやデータ保護、耐震強化等)、システム担当者等への教育訓

練、緊急時対応、それら取り組みの見直しに関する計画である。1995 年の阪神・淡路大震災を機に検討を進め、バックアップサイトの構築と同時に策定した。

・ 当該計画は、3～4 年の頻度で見直しを行っている。

・ システム関連部門で所掌しているその他のシステムを対象とした IT-BCP は、少しずつ議論を進めているものの、現時点では具体化はしていない。委員会において総合的な BCP が策定され、その方針を受けてシステム関連部門からユーザ部門に対し、IT-BCP の必要性の議論について働きかけをしていく予定である。

＜策定体制＞

・ システムを利用する組織加盟各社が構成員となっている委員会において策定している。

＜教育訓練や演習の実施と内容＞

・ 緊急時対応計画等が策定されているシステムに関する計画発動時の演習は、毎年 1 回実施している。メインサイトが設置されている地域とバックアップサイトが設置されている地域とで交互に実施している。システムの運用（特に復旧）に係る組織から各 1～2 名程度が参加している。昨年度は某県で大規模地震が発生したというシナリオを作成して演習に臨んだ。

② 重要業務と継続戦略

a. 重要業務

＜選定した重要業務＞

・ サービス利用者の契約者情報を管理するシステム。

b. 業務選定の理由・経緯

＜選定の理由や判断基準＞

・ 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。

＜戦略検討の方法＞

・ 大規模地震等によりメインサイトの利用ができない場合を想定している。

＜設定した目標＞

・ 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。

③ 重要業務のためのシステムの概要

a. 規模

・ メインサイト：メインフレーム（商用データセンタに設置）

・ バックアップサイト：メインフレーム（商用データセンタに設置）

b. システム構成と復旧対策の概要

・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。

＜この構成を採用した理由や判断基準＞

・主に想定しているリスクは地震であり、メインサイト立地地域に大規模地震が発生しても、当該地震による深刻な影響が及ばないと考えられる地域にバックアップサイトを準備している。

・データの更新頻度は月に 1 回であるため、バックアップサイトにデータを保管するためにネットワークは利用していない。

・システム構成の概要を図 4-102 に示す。

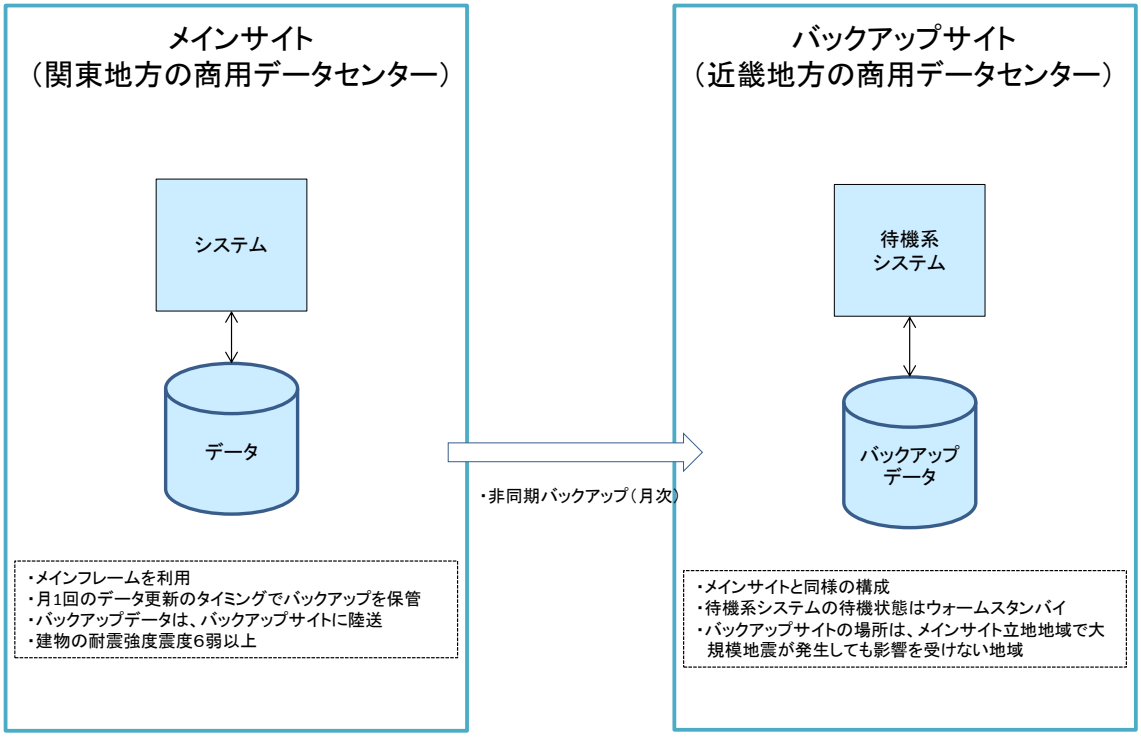


図 4-102 システム構成の概要

c. 技術的特徴

＜ポイント＞

・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（ウォームスタンバイ）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。

④ システム復旧対策のポイントと留意点

a. 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等の被害拡大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。

b. ポイント

・ 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。

c. 留意点や将来構想

・ 今回の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。
・ BCP が策定された時点で、他のシステムも含めた IT-BCP の検討を実施する予定である。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-18 のとおりである。

表 4-18 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		目標復旧水準（業務停止時）	RPO（目標復旧時点）	障害発生時点
			RTO（目標復旧時間）	24 時間以上
			RLO（目標復旧レベル）	特定業務のみ
		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
	耐障害性	サーバ	冗長化（機器）	ウォームスタンバイ
			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
		ネットワーク機器	冗長化（機器）	非冗長化
			冗長化（コンポーネント）	非冗長化
		ネットワーク	回線の冗長化	非冗長化

大項目	中項目	小項目	指標	対策
			経路の冗長化	非冗長化
		ストレージ	冗長化(機器)	特定の機器のみ冗長化
			冗長化(コンポーネント)	非冗長化
			冗長化(ディスク)	非冗長化
		データ	バックアップ方式	オフラインバックアップ
			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)
	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
		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
			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
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
			監視間隔	リアルタイム監視(分間隔)
	保守運用	定期保守頻度	定期保守頻度	週 1 回
		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
	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
		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
			駆けつけ到着時間	保守員到着が異常検知から数時間内
			SE 到着平均時間	SE 到着が異常検知から数時間内
		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
			予備機の有無	一部予備機あり
	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
	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
		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
		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
		定期報告会	定期報告会実施頻度	四半期に 1 回
			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
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
		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(電源確保可能時間は非回答)

(11) K 団体

① 事業の特徴と IT

a. 業種・企業概要

・ 業種:地方公共団体

・ 職員数:5,000 名強

b. 全社レベルの IT ガバナンス

＜経営戦略と IT の活用の関係＞

・ 基本計画に沿って、情報化分野の実施計画である情報化推進計画を策定し、情報化施策を総合的、計画的に進めている。

・ 昨今では IT 利用を前提として制度や業務が決められ、IT はあるのが当たり前の存在となっている。住民数が多いため、住民情報を職員の人手で管理するのは非現実的であり、IT を使わなければ業務が成り立たない。

＜IT 投資＞

・ 2012 年度の全組織における IT 関連当初予算は総額 32 億円である。IT 関連予算は年々減少しており、5 年間で 20～30%削減されている。

＜IT を活用して得られた効果＞

・ IT 活用の効果は、業務の効率化といったことには留まらない。IT 化を始めた当初は、紙台帳の電算化といった程度での活用であり、その効果も業務効率化が中心であった。しかし、平成 10 年頃からは、住民にインターネットを使ってサービスを提供する電子自治体の取組みが開始され、住民サービスの向上効果も上がっている。

・ 業務で IT を活用することで、情報の正確性も担保される。大量な情報を正確に処理できることで、提供すべき行政サービスが必要な住民へ提供されないといった漏れの発生も減り、公平性担保にもつながる。

＜IT の活用を促進する推進体制＞

・ 情報化推進体制として、副首長を CIO に任命し、「情報システム推進委員会」を設置している。情報システム推進委員会は政策経営部門の長をトップとして、各業務分野における計画担当課長、労働組合代表者等が委員となって構成されており、情報システム導入評価と情報セキュリティ対策の推進に関する審議を行っている。実務面では、情報システム部門が全庁的な情報化施策の調整を行うと共に、PMO としてシステム導入時の品質・コスト・スケジュール等の管理支援を行っている。

・ IT-BCP は情報システム部門情報化推進担当の職員が作成した。実装は主に情報システム部門基盤担当の職員が受け持っており、作成時の考えを受け継いで業務にあたっている。

c. BCP の策定とマネジメント

・ 災害対策部門にて、業務継続計画（震災編）を 2010 年 11 月に策定した。定期的な見直し時期は定めていないが、必要に応じ、実態に合わせた見直しは行っている。BCP は県の地震被害想定を元に作成されていることから、県の被害想定の見直しを受けて、今後見直しを図ると考えられる。

・ 震災発生時、情報システム部門は危機管理部門が中心となって設置される災対統括部に入り IT 部分の復旧業務を担う。このような立場から、BCP 作成にあたっても情報システム部門の情報化推進担当が検討メンバとして参加した。BCP のうち IT 基盤の現状分析、被害想定や復旧の考え方については、情報システム部門の職員が作成した（全体の 5%程度）。

・ 対象リスクは震災を想定している。

d. IT サービス継続計画（IT-BCP）の策定とマネジメント

＜策定時期と見直しの頻度＞

・ IT-BCP は 2010 年 3 月に策定した。毎年の進捗状況をもとにした施策の見直し、人事異動による連絡体制図の改訂など、実態に合わせたメンテナンスを毎年行っている。

＜策定体制＞

・ 震災時の情報システム復旧は情報システム部門に一任されているため、IT-BCP は情報システム部門長をはじめとする情報システム部門内で相談した。ただし、最終決定は、CIO が行っている。

＜対象リスク＞

・ 対象リスクとしては、全庁の BCP と同様に震災を想定している。

＜計画の構成・内容＞

・ IT-BCP の内容としては、以下が含まれている。

〇事業継続のために重要となる業務の維持に必要な IT サービスの特定
〇重要業務の目標復旧時間（RTO）を考慮した、IT サービスの目標復旧時間（RTO）
〇IT サービスの中断・停止に備えた事前対策を定めた対策実施計画
〇IT サービスの中断・停止に備えたシステム担当者等の教育訓練計画
〇IT サービスの中断・停止の場合の事後対策計画や緊急時対応計画
〇継続的な維持改善を行うための管理方法を定めた維持改善計画

・ 詳細なビジネスインパクト分析（BIA）は実施していない。現状の IT-BCP では、建物、電気、通信、情報システムなど資源別に「現状」「課題」「対策の方向性」をまとめるに留まっている。

・ 各部門が特定分野に限定して分析するというのは可能だろうが、情報システム部門がすべての行政サービスを対象に整理するのは、組織間の調整も困難であると考えられるため実現は難しい。

・ 震災時に限定し、発災から時系列に沿って業務の重要性を示すことは可能かもしれないが、通常時においてどの業務が重要かといったことを決めるのは、行政の立場では難しい（どの業務も重要であるという考え方になる）。

＜教育訓練の内容＞

・教育訓練は、全庁での防災訓練の一部として行っており、防災行政無線の伝達訓練、自家発電機の給油・駆動訓練などを行った。

＜BCP との連携＞

・IT-BCP は BCP より策定時期は早いが、同時進行で作成しており、内容については連携をとっている。IT-BCP に示された想定被害は BCP に基づいたものであり、IT-BCP の目標復旧時間（RTO）は、BCP に示された重要業務の目標復旧時間（RTO）を考慮した上で定めている。

・情報システム部門情報化推進担当は、全庁の BCP 策定にも関わっており、IT-BCP 作成に当たって、BCP との連携を取っている。

② 重要業務と継続戦略

a. 重要業務

・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捉え、そのために利用する「IT 基盤」を IT-BCP の対象システムとした。ここで IT 基盤とは、全庁ネットワーク（LAN、WAN）とネットワーク機器類、アクティブディレクトリ（認証基盤）、メール・グループウェア、ファイルサーバ、公開用 Web サーバ等を指している。

・住民情報系基幹システムは IT-BCP の直接の対象とはしていない。しかし、全庁の 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おり、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、必要な対策を実施している。

b. 業務選定の理由・経緯

・IT-BCP は震災をリスクとして想定しているため、地震発生後 3 日程度は、被災状況の把握や住民の安否確認、避難所・食糧・ライフラインに関する住民への情報提供といった災害対応を重要業務としている。

・IT 基盤は地震発生直後から利用する機能であると同時に、すべてのシステムの土台になるものであるとの考え方に基づき、IT 基盤の復旧を優先している。

・住民情報を取り扱う住民情報系基幹システムは、保有する情報システムの中で非常に重要なシステムであるため、対象とすべきとの声も上がったが、地震発生直後は通常通りの窓口業務の必要性は低いと考えられるため、IT-BCP の対象とはしなかった。また、窓口業務を行うために住民情報系基幹システムを再稼働するにも、土台部分となる IT 基盤の復旧が不可欠であり、IT 基盤を最優先に復旧するべきと考えた。

・震災時の復旧は情報システム部門に一任されていたため、情報システム部門長をはじめとする情報システム部門内で検討を進めた。

c. 戦略の内容と検討方法

［目標復旧時間（RTO）］

・全庁の BCP において示された被害想定や復旧想定を元に検討している。例えば、BCP にて電源復旧に 3 日程度かかるという想定を示していることから、それを受けて IT-BCP では 1 週間を目標復旧時間（RTO）の目安とした。

・ネットワークの種類ごとに設定している。

・重要なネットワークにおける目標復旧時間（RTO）は 3 日から 1 週間未満。

・その他のネットワークにおける目標復旧時間（RTO）は概ね 1 週間～1 か月。

・ネットワークは、自設で構築している。そのため、大地震等により重要なポイントなる地点の電柱が倒れてしまうと、実際には、1 週間で復旧するのはむずかしいと考えている。

・一方、住民情報系基幹システムについては、BCP に基づき、2 週間程度と設定している。

［目標復旧レベル（RLO）］

・重要なネットワークにおける目標復旧レベル（RLO）は通常時における拠点の 50%程度。

・その他のネットワークにおける目標復旧レベル（RLO）は通常時における拠点の 50%程度。

［目標復旧時点（RPO）］

・メールサーバやファイルサーバ、公開用・内部用 Web サーバなどの目標復旧時点（RPO）は、障害・地震発生前日に設定している。

・目標復旧レベル（RLO）設定にあたっては、ポイントとなる拠点の何割が残されるかといった想定を行い、1 週間程度で自治体全域の何割が復旧できるといった計算を行ったが、本来であれば WAN ネットワークの復旧には一か月必要だと考えている。

③ 重要業務のためのシステムの概要

a. 規模

・メールサーバ・グループウェア、ファイルサーバ等の IT 基盤の利用者は職員約 5,000 名であり、サーバはおおよそ 50 台程度である。

b. システム構成と復旧対策の概要

・システム構成としては、メインサイトと同一拠点において、ホットスタンバイにより冗長化している。

・遠隔バックアップは行っておらず、バックアップサイトはない。メールサーバ・グループウェアは、地震発生前のデータ復旧が求められる性質のシステムではないため、データ保全はそれほど重視していない。ファイルサーバはバックアップが必要と考えられるが、容量が大きく費用が膨大であるため実現が困難である。

・サーバの冗長化・非冗長化の費用比較はしていない。これまでは、可用性が最重要課題であり、非冗長化は考えていなかった。委託先事業者に対しても、非冗長化の提案は求めていない。このような構成についても情報システム部門で判断した。

・データ保全の重要性といった点からは、IT-BCP に定めている IT 基盤よりも、むしろ住民情報系

基幹システムのデータの方が重要である。そのため、月一回バックアップデータを媒体により遠隔地へ送付しており、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 4-103 に示す。

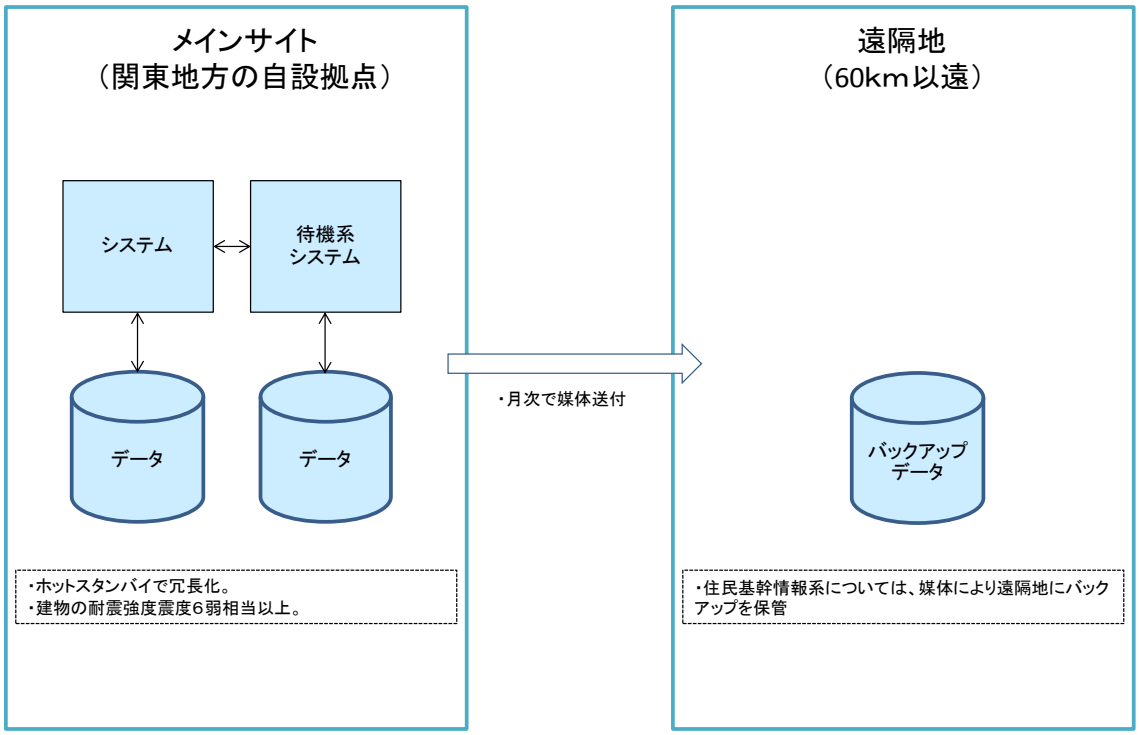


図 4-103 システム構成の概要

c. 技術的特徴

・仮想化サーバを昨年度以降導入している。仮想化により、将来的な外部データセンタへの業務委託の第一歩を進めたいと考えている。

・クラウド（SaaS）も検討中である。

④ システム復旧対策のポイントと留意点

a. 震災時等の効果

・現システムについて、被災経験はない。

b. ポイント

・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、緊急時に対応する職員用の食糧や工具、簡易トイレなどの備蓄を行っている。また、ソフト面での取り組みとしては、職員の外部研修受講も進めている。

・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。
・また、災害情報や避難物品の情報等を管理する防災情報管理システムは、本庁以外に、本庁と同時に被災しないと考えられる遠隔地のデータセンタに設置している。

c. 留意点や将来構想

・今年度、費用削減の観点からこのような現状を見直すため、システムのあり方を精査する予定である。住民情報系基幹システムなども含めた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。
・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。

⑤ システム復旧対策の詳細

システム復旧対策の詳細は表 4-19・表 4-20 のとおりである。

a. IT 基盤

表 4-19 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		目標復旧水準（業務停止時）	RPO（目標復旧時点）	IT-BCP では震災以外は定めていない。目標は障害発生直前。最悪でも 1 日前。
			RTO（目標復旧時間）	IT-BCP では震災以外は定めていない。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。
			RLO（目標復旧レベル）	IT-BCP では震災以外は定めていない。システムが治ったら復旧という認識であることから、100%といえる。
		目標復旧水準（大規模災害時）	システム再開目標	3 日から 1 週間
	耐障害性	サーバ	冗長化（機器）	IT 基盤系はほぼ全て冗長化されている
			冗長化（コンポーネント）	機器によって電源・UPS を冗長化している
		ネットワーク機器	冗長化（機器）	コアスイッチなど重要な機器のみ冗長化している
			冗長化（コンポーネント）	ごく一部の機器のみ冗長化している。今後の課題として認識している

大項目	中項目	小項目	指標	対策
		ネットワーク	回線の冗長化	WAN ネットワークは、自営網と事業者閉域網の併用により冗長化している。冗長化の範囲は徐々に拡大している。 LAN ネットワークは冗長化していない。
			経路の冗長化	冗長化している
		ストレージ	冗長化(機器)	ファイルサーバのストレージは冗長化している
			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
			冗長化(ディスク)	RAID1 による冗長化
		データ	バックアップ方式	オンラインバックアップしている
			データインテグリティ	エラー検出および再試行を実施
	災害対策	システム	復旧方針	バックアップサイトはない
		外部保管データ	保管場所分散度	分散保管していない
			保管方法	同一サイト内のストレージへのバックアップを行っている
運用・保守性	通常運用	バックアップ	バックアップ取得間隔	同期バックアップを行っている
			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
		運用監視	監視情報	エラー監視、リソース監視、パフォーマンス監視を行っている
			監視間隔	リアルタイム監視(秒間隔)を行っている
	保守運用	定期保守頻度	定期保守頻度	特定の一部機器のみ年に 1 度の点検を行っているが、却って障害がおこることがあるので、全ての機器は対象としていない
		予防保守レベル	予防保守レベル	保守委託先事業者からの提案により、一部の機器で行っている。検出はリアルタイムであるが、報告は定例会のときにまとめて実施されている。
	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している
		システム異常検知時の対応	対応可能時間	IT 基盤系は 24 時間対応である
			駆けつけ到着時間	連絡してから数時間以内の対応である。重要度の高くないシステムには、翌日対応のものもある。
			SE 到着平均時間	駆けつけ到着時間と同じ
		交換用部材の確保	保守部品確保レベル	保守契約に基づいて、規定年数の保守部品を確保している
			予備機の有無	予備機はない
	運用環境	マニュアル準備レベル	マニュアル準備レベル	組織の運用ルールに基づいて作成されたマニュアルを提供してもらっている
	サポート体制	一次対応役割分担	一次対応役割分担	従業員が障害の特定は行わず、委託先事業者へ連絡することを基本としているが、分かる範囲で一部は職員が対応している。 今後は、オンラインでエラー検知することで全て保守委託先事業者による対応としたい。
		サポート要員	ベンダ側対応者の要求スキルレベル	仕様では技術的スキル要件の保有を求めているが、細かく指定してはいない。実際には、事情に通じた人を期待している。システムによっては開発要員が常駐している。
		オペレーション訓練	オペレーション訓練範囲	起動停止のみであり、部品交換等の訓練は行っていない。実施可能時期が限られるため、復旧等の訓練は実施できていない(基幹システムにおいて実施したことはある)。
		定期報告会	定期報告会実施頻度	システムによって異なるが、基本的には月 1 回行っている
			報告内容のレベル	障害報告、運用状況報告を受けている。改善提案を受けるというよりは、報告会の場での協議である。
システム環境	機材設置環境条件	耐震/免震	耐震震度	耐震強度は 6 弱程度である。自庁データセンタは平成元年 2 月に竣工の設備である。
		電気設備適合性	停電対策	CVCF は 30 分強～1 時間弱。自家発電は 1 回の給油で 13 時間供給可能だが、システムにはつながっていない

b. 住民情報系基幹システム （参考）

表 4-20 システム復旧対策の詳細

大項目	中項目	小項目	指標	対策
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
		目標復旧水準（業務停止時）	RPO（目標復旧時点）	障害発生時点
			RTO（目標復旧時間）	4 時間以内
			RLO（目標復旧レベル）	処理性能が 50%程度となることを許容する
		目標復旧水準（大規模災害時）	システム再開目標	1 か月以内
	耐障害性	サーバ	冗長化（機器）	全てのサーバで冗長化
			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
		ネットワーク機器	冗長化（機器）	特定の機器のみ冗長化
			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
		ネットワーク	回線の冗長化	一部冗長化
			経路の冗長化	一部冗長化
		ストレージ	冗長化（機器）	全ての機器を冗長化
			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
			冗長化（ディスク）	RAID1 による冗長化
		データ	バックアップ方式	オンラインバックアップ
			データインテグリティ	非回答
	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
		外部保管データ	保管場所分散度	1 ヵ所(遠隔地)
			保管方法	媒体による保管
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
			監視間隔	リアルタイム監視（秒間隔）
	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
		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。
	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
		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
			駆けつけ到着時間	保守員到着が異常検知から数時間内
			SE 到着平均時間	SE 到着が異常検知から数時間内
		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
			予備機の有無	予備機無し
	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
	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
		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
		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
		定期報告会	定期報告会実施頻度	月 1 回
			報告内容のレベル	障害報告に加え運用状況報告を行う
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
		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

4.2.3　ヒアリング調査のまとめ

以上示したヒアリング調査の結果について、以下のようにまとめられる。

(1) 事業の特徴と IT

・調査対象企業等はいずれも IT 依存度が高いと認識している企業が多い。
・BCP や IT-BCP を文書化している企業等は少数であり、特にビジネスインパクト分析（BIA）を実施している企業等は少ない（実施中の社が 1 社のみ）。ビジネスインパクト分析（BIA）を実施していない理由としては、作業の負担が大きい、ノウハウ不足が挙げられる。
・システムの復旧対策は、情報システム部門が根拠となる考えや尺度を持ち、検討している。
・IT サービス継続において、IT-BCP の策定やビジネスインパクト分析（BIA）の実施が望まれるが、取り組みがある程度進んでいる企業にとっても容易ではなく、その実態を踏まえた有効な対策を検討する必要がある。

(2) 重要業務と継続戦略

・ビジネスインパクト分析（BIA）を実施しないで重要業務を定めている場合は、利益・売上高や顧客サービスへの影響、業界の規定や法令、災害時対応の緊急性等から定めている。
・ビジネスインパクト分析（BIA）を実施しないで復旧目標を定めている場合は、業界の規定、顧客との SLA、経験値、実現性等から定めている。
・復旧目標は、情報システム部門において検討し、経営層に諮っているケースが多い。
・上記のように、事例では、ビジネスインパクト分析（BIA）を行な、重要業務や復旧目標（IT サービス継続戦略の重要な要素）を実践的な手法により設定していた。事例でとられている手法は、実践的な手法として有益な知見であると考える。

(3) 重要業務のためのシステム基盤の概要

・事例では、認識しているリスクに最低限対応可能かつ投資可能な範囲で構成を決定している。
・過去に被災や障害等の経験がある企業等では、それを契機に対策を検討して、構成を決定している。
・これらの事例でとられている手法は、実践的な手法として有益な知見であると考える。

(4) 構築にあたってのポイントと留意点

・被災経験からは、人、データ、通信・電力、建物といった資源全般が喪失することへの備えが必要との教訓を得た。
・リスクを特定するのではなく、システムに関連する資源（リソース）の状態に基づき対策の発動を決定する例がある（資源に着目した、いわゆるリソースベースの対策を実施している）。

・　震災時の効果例としては、遠隔地保管されていたデータによりデータ復旧を果たしたれ、遠隔地の待機系システムに切り替えた例（ただし、念のためにとられた措置であり、同社にシステムには実被害はなし）があった。
・仮想化技術を導入し、サーバ統合化を進めながら、費用の増加を抑えてバックアップサイトを構築している例がある。
・ただし、自社開発のシステムを導入している例等で、安定稼働への不安やレスポンスが遅い等の理由から仮想化を導入していない場合もある。
・以上のように、事例からは、情報システムに関連する資源全般が喪失する可能性があることを前提に対策を実施することが重要であることと、そのために、資源に着目した対策を実施する事例とについて知見を得た。また新しい技術の活用が有効であるという知見を得た。

(5) システム復旧対策の詳細

・喪失が許されないデータを扱うシステムでは遠隔バックアップを実施している。
・大規模災害時に対して目標復旧時間を短く設定している企業等では、遠隔地に待機系システムを設置するとともに短い間隔でバックアップを実施している。
・被災時の通信確保の方策として衛星インターネットや、建物間通信用に無線 LAN 技術を適用するなど無線技術が有効に機能した例があった。
・事例からは、災害時に備えた遠隔地バックアップや遠隔地における待機系システムの整備を行うことの重要性、災害時の無線技術の活用等の有効性についての知見を得た。

5　考察　ー企業等の情報システム基盤の復旧能力の向上に向けてー

本章では、調査結果を踏まえ、企業等における情報システム基盤の復旧能力の向上を図るための取り組みの考え方ついて考察する。

5.1 調査結果全体のまとめ

IT サービス継続マネジメントの観点および技術的対策等の観点の両面から、調査結果の要点をまとめると、図 5-1 のように示せる。

	IT サービス継続マネジメントの観点	技術的対策等の観点
文献調査	✓ 震災を受け、IT サービス継続への意識は向上 ✓ BCP 策定への意識は高まっているものの、策定は進んでいない ✓ BCP 策定済企業においても事業継続マネジメントに満遍なく取り組めていない。特に教育訓練計画や維持改善計画	✓ 企業はバックアップ、通信・電力確保、復旧手順の確立が重要な対策と認識 ✓ 震災では多くの想定を超える被害が発生。通信・電力の広域的、長期的停止も発生 ✓ サーバ仮想化やクラウドによるバックアップサービスが復旧対策に有効
アンケート調査	✓ IT-BCP 策定済企業は 1/4 にとどまる ✓ 事業規模や IT 依存度が大きいほど取り組みは進んでいる ✓ IT-BCP 策定企業であっても IT サービス継続マネジメントに満遍なく取り組めていない。特にBIA、教育訓練計画、維持改善計画等 ✓ 取り組みが進んでいる企業は目標復旧時間（RTO）を設定 ✓ 戦略（RTO）と対策間で不整合が散見	✓ 事業規模や IT 依存度が大きいほど対策が充実 ✓ クラウド導入を検討している企業の目的の筆頭は災害対策 ✓ IT 依存度の高い企業でも遠隔バックアップの実施は約半数 ✓ 震災を踏まえ、データが毀損・滅失することへの懸念が高まっている ✓ 過去の震災やその他の障害等により、通信、電力の確保、データの消失、復旧手順書の不備が問題となった経験をした企業が多い
ヒアリング調査	✓ 調査対象には IT 依存度が高いと認識し対策が進んでいる企業も含まれるが IT-BCP を文書化している企業、BIA 実施企業は少数 ✓ しかし、多くの企業は、それぞれの考えと尺度から重要業務の決定と目標復旧時間（RTO）等を設定し、組織として有効と考えられる対策を決定、実施	✓ 喪失が許されない重要データを扱うシステムの多くは遠隔バックアップを実施 ✓ 被災経験から、人、データ、通信・電力、建物等資源全般の喪失に対する備えが必要との教訓 ✓ 情報システム基盤に関連する資源に着目した対策を実施 ✓ 仮想化技術を活用し、コスト増を抑えて有効に災害対策を実施している例

図 5-1　調査結果全体のまとめ（要点）

5.2 IT サービス継続マネジメントの観点

5.2.1 IT サービス継続マネジメントの確立と定着

企業等における情報システム基盤の復旧能力向上を図るためには、組織の中に IT サービス継続マネジメントの仕組みを確立していくことが望まれる。

東日本大震災を受け、IT サービス継続の取り組みの重要性は企業等に強く認識されている。この期を逸さず、IT サービス継続マネジメントについて、普及・啓発を図っていくことが望まれる。

IT サービス継続マネジメントの確立に向けては、「IT サービス継続ガイドライン」に示されるような IT サービス継続戦略の立案、IT サービス継続計画の立案、IT サービス継続体制の実装・運用・維持、IT サービス継続体制の監査、といった一連の取り組みが実施されることが望まれる。しかし、今回の調査結果からは、IT-BCP を策定している企業自体が少数であり、策定されている場合であっても、とりわけ、以下のような取り組みが実施されている例は少ない。

・ビジネスインパクト分析（BIA）の実施
・教育訓練計画の立案や実施
・維持改善計画の立案や実施

言い方を変えると、IT サービス継続の取り組みは、一定の実施がなされていたとしても、単に復旧対策として捉えられ、マネジメントシステムとしては十分に認識されていない可能性がある。

調査結果からは、企業等にとって、ビジネスインパクト分析（BIA）をはじめとする一連の取り組みを実施することは容易ではないことも明らかとなっている。事業継続や IT サービス継続に関するガイドラインや認証基準を活用し、マネジメントシステムの確立・運用に向けた継続的な活動を行っていくことが望まれる。

5.2.2 重要業務と復旧目標の明確化

先に示したように、企業等の IT サービス継続の取り組みの維持・向上を図るためには、IT サービス継続マネジメントを確立、定着していくことが望ましいが、その取り組みは容易ではない。まずは、その組織の IT サービス継続を図る上で、有効かつ実行できる範囲でシステム復旧対策を実施していくという考え方も重要である。

この点に関して、ヒアリング調査結果からは、ビジネスインパクト分析（BIA）が未実施、あるいは BCP や IT-BCP の策定を行っていない場合でも、組織それぞれの考え方や尺度を持って検討し、組織の IT サービス継続に有効と考えられるシステム復旧対策を実施している例が多くみられた。その場合、多くの例においては、以下の事項については、情報システム部門が経営層等とコミュニケーションをとりながら、組織として検討し決定していた。

・重要業務の検討と決定（守るべき業務はなにか）
・復旧目標の検討と決定（いつまでにどの程度復旧させるか）

アンケート調査結果からは、目標復旧時間（RTO）を設定している企業の方が、IT サービス継続における各取り組みを広範に実施している傾向が強いことが分かった。IT サービス継続における各取り組みは、経営層や事業部門を巻き込んでいく必要があり、システム復旧対策に対する動機付けがポイントとなってくる。一般的に、具体的な目標や指標は、複数の関係者と取り組みを推進する上で重要な役割を果たすことから、IT サービス継続における取り組みを広範に実施できている企業は、システム復旧対策の具体的な目標として、目標復旧時間（RTO）を有効に活用している例が多いと考えられる。

文献調査結果からも、重要業務や復旧目標を定めていない場合には、BCP が機能しない例が多いことが示されており、これらを定めることは事業継続を進める上で重要なポイントであることがわかっている。

IT-BCP の未策定企業が多い実態を踏まえると、まずは、このような IT サービス継続に取り組んでいく上で重要となる基本的な戦略を明確化するために重要業務と復旧目標を定め、対策を実施することが有効であると考える。

5.3 技術的対策等の観点

5.3.1 資源に対する代替策の検討の必要性

アンケート調査結果からは、事業の IT 依存度に応じて、システム復旧に関する対策が実施されていることが分かった。一方で、IT 依存度が高い企業であっても、遠隔地バックアップを実施している企業はほぼ半数にとどまるなど、十分に対策が実施されていない例があった。IT 依存度に応じて復旧対策を充実させていくことが必要である。

東日本大震災では、津波、原子力災害、被害の長期化・広域化等、従来想定していたリスクを超える「想定外」といわれる被害が多数発生した。

これを踏まえると、想定したリスクの範囲内で対策を実施するという考え方では限界があり、あらゆる情報システム基盤の構成要素が喪失する可能性があり得ると考える必要がある。その復旧対策としては、それらの資源を代替する対策を持つことが重要である。特に、文献調査やアンケート調査からは、データや通信、電力の喪失、復旧手順についての懸念が大きいことが示されている。また被災事例からは、これに加え、体制や建物、設備の確保が重要である、との教訓を得ている。今回の調査結果をもとに、情報システム基盤の構成要素別に、その対策のポイントを示す。

(1) 業務アプリケーション・業務データ

データは、バックアップがされていない限り代替するものがない。また独自開発したアプリケーション等についても同様である。今回の震災では、津波等により、施設全体が被災し、データが喪失する

被災事例があった。被災経験のある事例からも、データの保護は極めて重要であることが教訓として示されている。

調査事例では、重要データについて遠隔地バックアップを実施している例が多かった。しかし、文献調査やアンケート調査結果からは、IT 依存度の高い企業でも、重要データの遠隔地バックアップを実施している割合は少ない様子がうかがえた。重要データについては、遠隔地バックアップを進めることが重要と考える。なお、この点については、企業の遠隔地バックアップ実施意向も比較的高く、今後対策が進む可能性がある。

さらに目標復旧時間が数日内に設定されている等、目標復旧時間を短く設定している事例では、待機系システムの設置や遠隔地のバックアップサイトに同期バックアップを実施していた。目標復旧時間に応じて待機系システムの設置やバックアップサイトの設置も含めて対策を検討する必要がある。

(2) OS・ミドルウェア

OS やミドルウェア自体は、多くの場合、新たに調達することが可能ではあるが、必ずしも短時間に調達することができるとは限らず、特に災害時には円滑に調達できない可能性がある。また、環境設定を含めるとその復旧を短時間に実施することは困難である。

アンケート調査結果からは、システム(OS、アプリ、環境設定)についてのバックアップを実施している企業は半数ほどであった。復旧に備えてこれらのバックアップ、遠隔地バックアップも考慮する必要がある。また、復旧目標を短く設定している場合には、待機系システムの設置やバックアップサイトの設置も含めて対策を検討する必要がある。

(3) ハードウェア機器やネットワーク機器

機器については、多くの場合、新たに調達することが可能ではあるが、必ずしも短時間に調達することができるとは限らず、特に災害時には円滑に調達できない可能性がある。

事例では、たとえばテスト機を代替機として想定している例があった。また、目標復旧時間を短く設定している事例では、待機系システムやバックアップサイトを設置し、目標復旧時間内での復旧対策を実施している例があった。

代替機を用意することや、各企業の目標復旧時間に応じて、待機系システムの設置やバックアップサイトの設置も含めて対策を検討する必要がある。

(4) 建物、設備

今回の震災では、堅牢と考えられていた施設も津波で破壊される例があった。施設が失われることも考慮する必要がある。

代替施設を準備しておくことや、目標復旧時間にあわせて、バックアップサイトの設置も含めて対策を検討する必要がある。

(5) システム運用の体制や仕組み

① 体制

今回の震災では、システム担当者が被災し、復旧が困難になった事例があった。復旧対応の代替ができるよう、システム担当者を複数(兼務体制等も含め)置くことが望ましい。

また、システムに関連するドキュメントを整備し、他の要員が、より容易に復旧対応できるような環境を整えることが望まれる。

② システム運用の仕組み

文献調査結果からは震災を受けて復旧手順の見直しの必要性や震災時のデータ復旧時に問題があった点、またアンケート調査からは多くの企業で過去の障害・災害時の復旧手順に問題があった点が示されている。

復旧手順の整備や見直しは重要な対策として指摘できる。

(6) 通信・電力

① 通信

今回の震災では、通信サービスが広域的に、また長期的に遮断されるという状況が生じた。通信についても、遮断が長期化する前提で代替策を用意することが望まれる。

事例調査結果からは、回線の冗長化を図っている例の他、衛星インターネットや無線 LAN 技術を活用した建物間通信が復旧時に有効に活用された例があった。

企業等のネットワークの利用状況を踏まえ、回線の冗長化、多様化、無線技術の活用等の代替策を用意することが有効である。

② 電力

今回の震災では、震災による直接的な損壊に加え、電力不足による計画停電の発生等、電力供給サービスが広域的に、また長期的に遮断されるという状況が生じた。電力についても、遮断が長期化する前提での代替策を用意することが望まれる

事例調査結果からは、過去の停電の経験から自家用発電機を整備やデータセンタの利用、遠隔地にバックアップサイトを設けることにより計画停電の影響を回避した事例があった。

自家用発電機の用意、燃料の備蓄、データセンタの活用、異なる電力管内におけるバックアップサイトの設置等の対策が有効である。

以上の対策の要点を表 5-1 にまとめる。

表 5-1 東日本大震災を踏まえた主な対策(必要資源確保のための代替戦略)

<table>
<tr><th>構成要素</th><th colspan="3">対策</th></tr>
<tr><td>業務アプリケーション・業務データ</td><td>・重要データのついては遠隔地バックアップの実施。</td><td rowspan="3">・待機系システムの設置。</td><td rowspan="4">・バックアップサイトの設置。</td></tr>
<tr><td>OS・ミドルウェア</td><td>・遠隔地バックアップを含むバックアップの実施。</td></tr>
<tr><td>ハードウェア機器やネットワーク機器</td><td>・代替機の用意(テスト機の活用等も含む)。</td></tr>
<tr><td>建物、設備</td><td colspan="2">・代替施設の準備。</td></tr>
<tr><td>システム運用の体制や仕組み</td><td colspan="2">・システムに携わる要員の複数化(兼務要員の充当も含む)。
・システム関連ドキュメントの整備と遠隔地保管。
・復旧手順の整備。</td></tr>
<tr><td>通信</td><td colspan="3">・回線の冗長化、多様化。
・災害時等における衛星インターネット等の無線技術の活用。</td></tr>
<tr><td>電力</td><td colspan="3">・計画停電、長期間の停電に備えた自家発電機の整備、重油の備蓄、データセンタの活用。
・異なる電力管内におけるバックアップサイトの整備。</td></tr>
</table>

5.3.2 企業の実情等を踏まえた技術・サービスの有効活用

文献調査結果で示したように、システム復旧対策に関連して、サーバ仮想化技術やクラウドサービスの活用することが可能である。事例においてもサーバ仮想化技術を有効に活用している例が見られた。

システム復旧対策に求められる要件や、技術・サービスの留意点を勘案しながら活用することが有効である(表 5-2)。

表 5-2 新しい技術・サービス活用の考え方

技術・サービス	活用の考え方
サーバ仮想化技術	・サーバ仮想化環境下においては、従来技術と比較し、メインサイトの信頼性向上対策(二重化・クラスタリングに相当)・バックアップサイトの構築が容易に実現できる。 ・採用にあたっては動作保証、レスポンスの低下等の留意点も勘案する。
クラウドサービス	・遠隔バックアップ、データセンタ内のバックアップ、複数のデータセンタに配置するなど、災害対策に有効なサービスが登場しつつある。 ・機能制約、コスト、セキュリティ面等の留意点を勘案して活用を検討する。

5.4 IT サービス継続に関する基本的な戦略と具体的対策との整合性確保

前述のように、IT サービス継続マネジメントの観点からは、企業の取り組みにおいて、まずは以下の基本的な戦略を押さえる必要がある。

・重要業務の検討と決定（守るべき業務はなにか）

・復旧目標の検討と決定（いつまでにどの程度復旧させるか）

また、技術的対策等の観点からは、東日本大震災の経験を踏まえ、あらゆる構成要素が喪失する可能性があることに備え、リスクに関わらず必要な資源を代替する対策を検討・実施することが有効でると考える。あわせて新しい技術やサービスの活用も有効であると考える。

ヒアリング調査結果からは、IT サービス継続における基本的な戦略を定めた上で、有効と考えられる復旧対策を実施している事例が多くみられた。その際、基本的な戦略と整合のとれた復旧対策が実施されていた。

また、アンケート調査結果からは、設定している目標復旧時間に対して、実施している対策にギャップがあると考えられる企業が散見された。企業がこのようなギャップを認識していない場合、対策を実行したとしても障害時や災害時に目標どおりシステム復旧することはできず、想定していたとおりに事業を継続することはできない。

システム基盤の復旧能力の向上のためには、事業の IT 依存度や経営資源の制約等を踏まえ、最悪の事態を避けるために企業等として実施可能な対策を実施する必要がある。IT サービス継続の基本的戦略と復旧対策の関係を理解し、整合のとれた復旧対策を実施することが重要である。

以上の点をまとめると、企業等において情報システム基盤の復旧能力の向上を広く図っていくためには、各企業が IT サービス継続に関する基本的な戦略（重要業務と復旧目標を定める）を明確化するとともに、この基本的な戦略と整合性が確保できるよう、情報システム基盤に関連する資源についての代替策を選択して実施することが重要であると考える（図 5-2）。

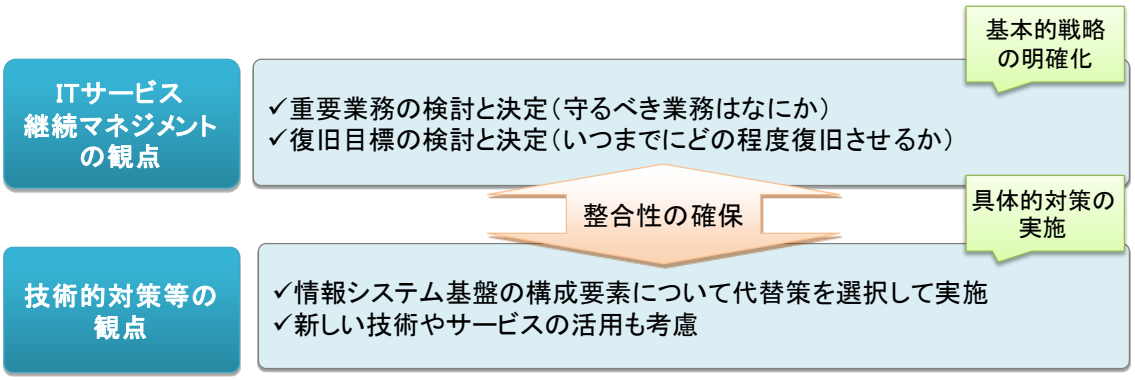


図 5-2　企業等におけるシステム復旧対策の取り組みのポイント

IPA が公表している「高回復力システム基盤導入ガイド」（以下「ガイド」という）は、ここで示した内容と同様の考え方で、復旧対策を実施することをめざしたものであり、基本的な戦略と対策の対応関係についても解説されている。このようなガイドを活用することで、企業のシステム復旧対策を進めていくことは有効であると考える。

6　付録

6.1 付録①　アンケート調査票

4.1に示したアンケート調査は、以下の調査票にて実施した。

貴社のプロフィールについてお伺いします。

✓ **全ての方にお伺いします**

ご質問項目	回答欄 （資本金等は直近の決算日の内容、業種・主な事業内容等は売上比率が最も大きい内容をご記載ください）
Q1.設立年月日	〔　　〕年　〔　　〕月　〔　　〕日
Q2.資本金 （一つ選択）	1. 1 億円未満 2. 1 億円～3 億円未満 3. 3 億円～5 億円未満 4. 5 億円～10 億円未満 5. 10 億円～50 億円未満 6. 50 億円～100 億円未満 7. 100 億円～300 億円未満 8. 300 億円～500 億円未満 9. 500 億円～1,000 億円未満 10. 1,000 億円以上 11. その他（　　）
Q3.本社所在地	〔　　〕都・道府・県　〔　　〕市・区町・村
Q4.拠点数 （一つ選択）	1. 1 拠点～5 拠点未満 2. 5 拠点～10 拠点未満 3. 10 拠点～30 拠点未満 4. 30 拠点～100 拠点未満 5. 100 拠点～300 拠点未満 6. 300 拠点～1,000 拠点未満 7. 1,000 拠点以上 8. その他（　　）
Q5.従業員数 （一つ選択）	1. 50 人未満 2. 50 人～300 人未満 3. 300 人～1,000 人未満 4. 1,000 人～5,000 人未満 5. 5,000 人～10,000 人未満 6. 10,000 人以上 7. その他（　　）
Q6.業種 （一つ選択）	1. 建設業 2. 製造業 3. 卸売・小売業、飲食店 4. 金融・保険業 5. 不動産業 6. 運輸・通信業 7. 電気・ｶﾞｽ・水道・熱供給業 8. サービス業 9. その他（　　）
Q7.主な 事業内容	〔　　〕
Q8.御社事業の IT 依存度 （一つ選択）	1. ほとんどの事業、業務が IT に大きく依存している 2. IT に依存している事業、業務が多い 3. IT に依存している事業、業務が少ない

ITサービス継続に関する取り組み状況についてお伺いします。

✓ **全ての方にお伺いします**

ご質問項目	回答欄（当てはまるもの 1 つに○を付けてください）
Q9.事業継続計画	1. 策定済み　2. 未策定（検討中） 3. 未策定（予定なし）　4. 不明　5. その他（　　）
Q10.IT 部門における、事業継続計画（IT サービス継続計画、IT-BCP）	1. 策定済み　2. 未策定（検討中）　⇒Q11～Q14 へ 3. 未策定（予定なし）　4. 不明 5. その他（　　）　⇒Q15 へ

✓ **Q10 で「1. 策定済み」又は「2. 策定中（検討中）」と回答した方にお伺いします。**

ご質問項目	回答欄（もっとも当てはまるものに一つずつ○をつけてください）			
Q11. IT サービス継続に関して、貴社では以下の取り組みを組織として実施していますか。	実施している	実施を検討中	実施していない	不明
Q11-1 事業継続のために重要となる業務の維持に必要なIT サービスを特定している	1	2	3	4
Q11-2 ビジネスインパクト分析(業務影響度分析)を実施している	1	2	3	4
Q11-3 重要業務の目標復旧時間等を考慮して、IT サービスの目標復旧時間等を定めている	1	2	3	4
Q11-4 IT サービスの中断、停止に備えた事前対策(代替システムやデータ保護、耐震強化等)を定めた対策実施計画を策定している	1	2	3	4
Q.11-5 IT サービスの中断、停止に備えた、システム担当者等の教育訓練内容を定めた教育訓練計画を策定している	1	2	3	4
Q.11-6 IT サービスが中断、停止した場合に、復旧するための対応体制、手順等を定めた事後対策計画や緊急時対応計画を策定している	1	2	3	4
Q.11-7 IT サービス継続の取り組みの継続的な維持改善を行うための管理方法を定めた維持改善計画を策定している	1	2	3	4

ご質問項目	回答欄	
Q12.IT サービス継続計画策定時に想定するリスク（複数選択可）	1. 自然災害(直下型地震による局所被害) 2. 自然災害(大規模地震による広域被害) 3. 自然災害(津波) 4. 自然災害(その他、竜巻や高潮等) 5. ｲﾝﾌﾙｴﾝｻﾞや感染症等によるﾊﾟﾝﾃﾞﾐｯｸ 6. 建物や施設の破壊・損失 7. 原子力災害 8. 社会的ｲﾝﾌﾗの障害(通信回線関連以外) 9. ハードウェアの故障	10. ソフトウェアの不具合 11. システムの処理能力オーバーフロー 12. 通信回線関連の故障 13. 停電 14. 外部コンピュータシステムの故障 15. テロやサイバー攻撃等の外部からの攻撃 16. 特に定めていない 17. 不明 18. その他(　　)
Q13.重点的に取り組んでいる領域（複数選択可）	1. 耐震構造の建物やバックアップサイト 2. 冗長化された電源供給やネットワーク 3. 情報処理設備や機器の冗長化 4. OS 等やデータの冗長化	5. データの遠隔地保管 6. システム運用の仕組みや体制 7. 不明 8. その他(　　)
Q14.リカバリ要件定義やバックアップポリシー策定の際に参照した規格やガイドライン等（複数選択可）	1. IT サービス継続ガイドライン(経産省) 2. JISQ20000-1、JISQ20000-2 3. ITIL 4. 金融機関等のシステム監査指針 5. 金融機関等コンピュータシステムの安全対策基準・解説書 6. PAS77：2006,(BSI) 7. 非機能要求グレード(IPA) 8. 事業継続ガイドライン(内閣府) 9. 企業における情報セキュリティガバナンスのあり方に関する研究会報告書 参考資料　事業継続計画策定ガイドライン(経産省)	10. Good Practice Guidelines(BSI) 11. 金融機関等におけるコンティンジェンシープラン策定のための手引き 12. BS25999-1:2006、BS25999-2:2007 13. NIST SP800-34 14. ISO PAS 22399:2007, 15. ISO/IEC27001,27002/JISQ27001,2700 16. ISO/IEC17799 17. NIST SP800-53 18. ISO/IEC,TR18044 19. ISMS ユーザーガイド(JIPDEC) 20. その他(　　)

現在利用しているコンピュータシステムと新しい技術の採用状況についてお伺いします。

✓ **全ての方にお伺いします**

ご質問項目	回答欄
Q15.コンピュータシステムを運用している業務（複数選択可）	1. 財務・会計　4. 調達　7. 販売 2. 人事・給与　5. 生産・サービス提供　8. カスタマーサポート 3. 開発・設計　6. 物流　9. その他（　　）
Q16. Q15 の業務で運用しているシステムのうち、事業継続において最も影響の大きいシステム（複数選択可）	1. 財務・会計管理システム 2. 人事管理システム 3. 販売管理システム 4. 生産管理システム 5. 物流・在庫管理システム 6. 勘定系システム 7. 開発管理システム 8. 設備管理システム 9. 企業間連携システム 10. Web 上の個人向けサービス提供システムや販売サイトのシステム（SNS、ｼｮｯﾋﾟﾝｸﾞｻｲﾄ等） 11. 顧客管理システム 12. 分析系システム（BI/DWH） 13. 営業支援システム（SFA） 14. メール・グループウェア 15. 社内向けホームページ 16. 社外向けホームページ 17. 運用・セキュリティ関連システム 18. その他（　　）
Q17.データの保管（バックアップ）対象となっているシステム	Q16 で選択したシステムのうち該当する番号 1～18 を本欄に記載（複数選択可）

✓ **全ての方にお伺いします（Q16でお伺いした事業継続において最も影響の大きいシステムについてお答えください）**

ご質問項目	回答欄
Q18.仮想化技術の利用状況（一つ選択）	1. 利用している　2. 利用していない（検討中）　⇒Q19 へ 3. 利用していない（予定無し）　4. 不明　⇒Q20 へ

✓ **Q18. で「利用している」、「2. 利用していない（検討中）」の方にお伺いします**

ご質問項目	回答欄
Q19.仮想化技術の導入対象（複数選択可）	1. サーバ　2. ストレージ　3. ネットワーク　4. クライアント端末 5. その他（具体名　　）

✓ **全ての方にお伺いします（Q16でお伺いした事業継続において最も影響の大きいシステムについてお答えください）**

ご質問項目	回答欄		
Q20.クラウドサービスの利用状況（一つ選択）	1. 利用している	2. 利用していない（検討中）	⇒Q21～Q22 へ
	3. 利用していない（予定無し）	4. 不明	⇒Q23 へ

✓ **Q20. で「利用している」、「2. 利用していない（検討中）」の方にお伺いします**

ご質問項目	回答欄	
Q21.クラウドサービスの導入目的（複数選択可）	1. 導入費用の低減 2. 運用・保守費用の低減(機器の削減、料金の削減など) 3. 運用要員の削減・負担軽減 4. サービス提供開始期間の短縮 5. 運用費用の変動費化（不要の際に即座に利用を停止するなど） 6. 試験的な導入 7. パソコン、携帯電話、スマホなど多様なユーザ端末への対応	8. 災害への対策 9. 最新の情報技術の利用 10. 優れたアプリケーションの活用 11. データ容量やレスポンス応答などピーク時対応の外部化（ピーク時対応をクラウド事業者に任せる） 12. 高いセキュリティの確保(アカウント管理,データ保護,信頼性など) 13. その他（　　）
Q22.利用中のクラウドサービスの種類（複数選択可）	1. SaaS（ソフトウェアをサービスとして提供） 2. PaaS（アプリケーションを稼働させるための基盤（プラットフォーム）をサービスとして提供） 3. IaaS（サーバ、CPU、ストレージなどのインフラをサービスとして提供） 4. RaaS（システム回復を目的としたクラウド上のシステムやデータのバックアップ・リカバリサービス） 5. DaaS（クラウドを利用したデスクトップ環境の仮想化） 6. その他（具体名称や概要：　　）	

システム構成についてお伺いします。
※Q16でお伺いした事業継続において最も影響の大きいシステムについてお答えください

✓ **全ての方にお伺いします**

ご質問項目	回答欄	
Q23.システム（サーバ）の冗長化の状況（複数選択可）	1. 同一サイト（メインサイト）内に待機系システムを設置している 2. バックアップサイト（遠隔地）に待機系システムを設置している	⇒Q24～Q25 へ
	3. 冗長化していない　4. 不明 5. その他（　　）	⇒Q26 へ

✓ **Q23で「1. 同一サイト（メインサイト）内に待機系システムを設置している」又は「2. バックアップサイト（遠隔地）に待機系システムを設置している」と回答した方にお伺いします**

ご質問項目	回答欄	コールドスタンバイ	ウォームスタンバイ	ホットスタンバイ	不明
Q24.待機系システムの状態（一つずつ選択）	Q24-1.同一サイト（メインサイト）	1	2	3	4
	Q24-2.バックアップサイト（遠隔地）	1	2	3	4

※コールドスタンバイ（電源投入や設定等がなされていない状態で待機）、ウォームスタンバイ（障害発生時に一定の作業で切り替えられる状態で待機）、ホットスタンバイ（本番システムと同様の構成で起動し待機）

ご質問項目	回答欄	一部自動化	全て手動	不明
Q25.障害発生時の復旧作業の自動化の状況（一つずつ選択）	Q25-1.同一サイト（メインサイト）	1	2	3
	Q25-2.バックアップサイト（遠隔地）	1	2	3

リカバリ要件定義の有無と内容についてお伺いします。
※Q16でお伺いした事業継続において最も影響の大きいシステムについてお答えください

✓ **全ての方にお伺いします**

ご質問項目	回答欄 1	回答欄 2：回答欄 1 で「1. 策定済み」または「2. 未策定（検討中）」を選択した方のみ選択肢からもっとも近い設定条件を選択してください。その他には内容を記載ください ※多段階に設定している場合は第一段階の条件を選択してください
Q26.目標復旧時間（RTO）の設定（一つずつ選択）	1. 策定済み 2. 未策定（検討中） 3. 未策定（予定無し） 4. 不明	① 1 分程度～10 分未満 ② 10 分～30 分未満 ③ 30 分～1 時間未満 ④ 1 時間～6 時間未満 ⑤ 6 時間～24 時間未満 ⑥ 1 日～3 日未満 ⑦ 3 日～1 週間未満 ⑧ 1 週間～1 か月未満 ⑨ 1 か月～3 か月未満 ⑩ 3 か月以上. ⑪ 不明 ⑫ その他（　　）
Q27.目標復旧レベル（RLO）の設定（一つずつ選択）	1. 策定済み 2. 未策定（検討中） 3. 未策定（予定無し） 4. 不明	① 障害・被災前と同等の業務を実施できる水準 ② 障害・被災前より低い性能（パフォーマンス）水準（処理速度が通常の 6 割、等） ③ 障害・被災前より業務・機能を制限した水準（購買履歴の閲覧のみ可能、等） ④ 障害・被災前より利用できる場所や端末を制限した水準（本社の 1 部の端末のみ利用可等） ⑤ 不明　⑥ その他（　　）
Q28.目標復旧時点（RPO）の設定（一つずつ選択）	1. 策定済み 2. 未策定（検討中） 3. 未策定（予定無し） 4. 不明	① 障害・被災発生の直前まで復旧 ② 障害・被災発生の前日まで復旧 ③ 障害・被災発生の 1 週間前まで復旧 ④ 障害・被災発生の 1 か月前まで復旧 ⑤ 不明　⑥ その他（　　）

※目標設定時間：RTO＜Recovery Time Objective＞、業務を復旧するまでの目標時間
目標復旧レベル：RLO＜Recovery Level Objective＞、復旧させる目標水準
目標復旧時点：RPO＜Recovery Point Objective＞、データ損失の最大許容範囲

データの保管（バックアップ）状況についてお伺いします。
※Q16でお伺いした、事業継続において最も影響の大きいシステムについてお答えください

✓ **全ての方にお伺いします**

ご質問項目	回答欄	
Q29.データの保管（バックアップ）の実施状況 （一つ選択）	1. 実施している	⇒Q30～Q42 へ
	2. 実施していない　3. 不明 4. その他（　）	⇒Q43 へ

✓ **Q29で「1. 実施している」と回答した方にお伺いします**

ご質問項目	回答欄
Q30.バックアップポリシーの明確化 （一つ選択）	1. 全社的にガイドラインを定めており、全部又は一部のシステム毎に明確化している 2. 全社的にガイドラインを定めているが、個別のシステムのバックアップポリシーには反映していない 3. 全社的なガイドラインは無いが、全部または一部のシステム毎に明確化している 4. 明確化していない　5. 不明 6. その他（　）
Q31.バックアップ対象 （複数選択可）	1. データ（データベース関連のデータ） 2. データ（上記以外、ドキュメントや画像ファイル等） 3. システム（OS、アプリケーション、環境設定ファイル等 4. 不明　5. その他（　）
Q32.バックアップの実行単位 （複数選択可）	1. バックアップ対象毎に別々にバックアップ（例：データとシステムは別々にバックアップ） 2. 物理サーバ全体を、イメージバックアップしている 3. 仮想サーバ環境で、VM 単位でイメージバックアップしている 4. 仮想サーバ環境で、ストレージ単位でイメージバックアップしている。 5. 不明　6. その他（　）
Q33.データの完全性 （一つ選択）	1. データの完全性や復旧時のエラー検出に関する要件を定めている 2. 定めていない　3. 不明　4. その他（　）
Q34.バックアップの方式 （一つ選択）	1. システムを停止してバックアップしている（オフラインバックアップ） 2. システムを停止せずにバックアップしている（オンラインでバックアップ） 3. 上記 1 と 2 を組み合わせて実施している 4. 不明　5. その他（　）
Q35.バックアップの頻度 （複数選択可）	1. リアルタイムバックアップ 2. 週 1 回のフルバックアップ＋日次での差分／増分バックアップ 3. フルバックアップ⇒（頻度を選択：①日次、②週次、③月次） 4. その他（　） ※複数の対象をバックアップしている場合は、最も代表的なものをお答えください。
Q36.バックアップの世代管理 （複数選択可）	1. 1 世代　3. 3 世代　5. 5 世代　7. 不明 2. 2 世代　4. 4 世代　6. それ以上　8. その他（　）
Q37.バックアップしている媒体（メディア）	1. 磁気テープ　4. 外付けハードディスクドライブ　7. その他（　） 2. 光学ディスク　5. ストレージ装置 3. USB フラッシュメモリ　6. 不明
Q38.バックアップの保管場所の分散度 （複数選択可）	1. 本番システムが設置されている拠点と同一拠点 2. 別拠点（本番システムが設置されている拠点との距離が 60Km 未満） 3. 別拠点（本番システムが設置されている拠点との距離が 60Km 以上） 4. 不明　5. その他（　）

ご質問項目	回答欄
Q39.異なる拠点でバックアップを保管する場合のバックアップの取得間隔（複数選択可）	1. リアルタイム 2. 非同期　⇒（頻度を選択：①日次、②週次、③月次・その他[　　]） 3. 異なる拠点に保管していない 4. 不明　　5. その他（　　） ※複数拠点で保管している場合は、該当するもの全てをお答えください
Q40.バックアップデータの施錠管理状況（複数選択可）	1. 保管している建物に施錠 2. 保管しているフロアに施錠 3. 保管している部屋に施錠 4. 保管している筐体（棚・耐火金庫等）に施錠 5. 外部のデータ保管サービスを利用 6. 不明 7. その他（　　） ※複数個所に保管している場合は、該当するものを全てお答えください
Q41.バックアップデータの暗号化（一つ選択）	1. 全てを暗号化している 2. 一部を暗号化している 3. 暗号化していない 4. 不明 5. その他（　　）
Q42.バックアップ作業の自動化の範囲（一つ選択）	1. 全てのバックアップ作業を自動化している 2. 一部のバックアップ作業を自動化している 3. バックアップ作業は手動で実施している 4. 不明 5. その他（　　）

震災被害の経験とその後の対応についてお伺いします。

✓ **全ての方にお伺いします**

ご質問項目	回答欄
Q43.情報システムの利用を制限された経験のある震災（複数選択可）	1. 東日本大震災［2011.3］ 2. 新潟県中越大震災［2004.10］ 3. 阪神淡路大震災［1995.1］ 4. その他震災[直近 15 年程度]（　　） 5. 不明 6. 経験はない
Q44.東日本大震災等の震災後の、データの保管（バックアップ）に対する認識の変化（一つ選択）	1. 震災前の対策では不十分だと認識し、対策の検討を開始した　⇒Q45～Q46 へ 2. 震災前の対策では不十分だと認識したものの、対策の検討には至らなかった 3. 震災前の対策で十分だと認識し、現状維持とした　⇒Q47 へ 4. 不明　　5. その他（　　）

✓ **Q44で「1. 震災前の対策では不十分だと認識し対策の検討を開始した」と回答した方にお伺いします**

ご質問項目	回答欄
Q45.震災で経験した又は今後懸念する、データの保管（バックアップ）に関する被害や問題（複数選択可）	1. メインサイトシステムのデータの滅失 2. メインサイトシステムのソフトウェアの滅失 3. バックアップ（データ）の滅失 4. バックアップ（ソフトウェア）の滅失 5. バックアップの復元に時間がかかる 6. バックアップデータの欠損が生じる 7. バックアップデータの完全性が確保されない 8. 緊急時にバックアップデータの活用が困難（機密性確保対策が厳格過ぎる） 9. 不明 10.その他（　　）

Q46. 震災後に検討を開始したデータの保管（バックアップ）に関する対策（複数選択可）	1. バックアップポリシーの策定や見直し 2. バックアップ対象の見直し 3. バックアップの実行単位の見直し 4. データインテグリティ（データの完全性やエラー検出に関する要件）の見直し 5. バックアップ方式の見直し 6. バックアップの頻度（フル、差分／増分バックアップ）の見直し 7. バックアップの世代管理の見直し 8. バックアップの保管媒体の見直し 9. バックアップの保管場所の分散度の見直し 10. バックアップの取得間隔の見直し 11. バックアップの施錠管理方法の見直し 12. バックアップの暗号化方法の見直し 13. 不明 14. その他（　　）
具体的なソリューション等がある場合は、右欄に可能な範囲でご記載ください	＜例：重複排除機能、SnapRestore 機能（SnapShot を利用した高速リカバリ機能）、ストレージベースレプリケーション（ストレージ間の高速データコピー機能）等＞

その他復旧に関する事項についてお伺いします。
※東日本大震災に限らず、システム復旧全般についてご回答ください

✓ **全ての方にお伺いします**

ご質問項目	回答欄
Q47.過去に、システムの復旧において、問題となった事項（複数選択可）	1. 代替拠点を確保できなかった 2. 電源を確保できなかった 3. 重油を確保ができなかった 4. 通信を確保できなかった 5. 復旧要員（自社）を確保できなかった 6. 復旧要員（外部委託事業者）を確保できなかった 7. 設備・機器等の資材を確保できなかった 8. 必要なデータの消失 9. ソフトウェアの消失 10. 非常時の体制への切り替え（BCP発動）が円滑にできなかった 11. 必要なデータが厳重に管理されていたため（施錠や上長承認手順の義務化等）、データへのアクセスができなかった 12. 必要なデータが暗号化されており、復号化できなかった 13. 必要なデータが保管されていなかった（揃わなかった） 14. 復旧手順書が未整備、手順が不明確 15. 復旧手順書の所在が不明 16. 復旧手順書の内容の不備 17. 復旧手順書どおりにシステムが動作しない（システムの技術的不備） 18. 復旧手順書どおりに作業できない（要員のスキル・習得不足） 19. 優先的に復旧するシステムが不明確 20. システム間の関係の考慮不足で、システムを優先順序どおりに復旧できない 21. バックアップ系から、本番系へ戻すこと（フェイルバック）が円滑にできない 22. 外部委託事業者との契約条件の不足や不備 23. 不明 24. その他（　　）
Q48.システム復旧に有効であった技術・サービス（複数選択可）	1. 仮想化技術 2. クラウドサービス（SaaS、PaaS、IaaS） 3. RaaS（システム回復を目的としたクラウド上のシステムやデータのバックアップ・リカバリサービス） 4. DaaS（クラウドを利用したデスクトップ環境の仮想化） 5. データセンタ 6. 無線等を使った通信サービス 7. 省電力技術 8. その他（　　）

以上

6.2 付録② 情報システム基盤の復旧に関する対策に資する国際規格やガイドライン

6.2.1 対象分野

情報システム基盤の復旧に関する対策に資する主要な国際規格やガイドライン及びそれらの関連性を整理した。対象分野は、「事業継続」や「IT サービス継続」、「リスクマネジメント」、「その他（IT サービス管理）」である。

6.2.2 国際規格やガイドラインの関連図

各分野は相互に関連しており、直接的な参照が無い場合でも、考え方等が反映されている場合がある。図 6-1 は、分野毎の国際規格やガイドラインを時系列に配置し、関連していると考えられる規格間を線で結んだ図である。各規格間を結ぶ線は、必ずしも引用規格または参考文献として記載されているものではなく、策定にあたり影響を与えたと考えられる場合に記載していることに留意いただきたい。

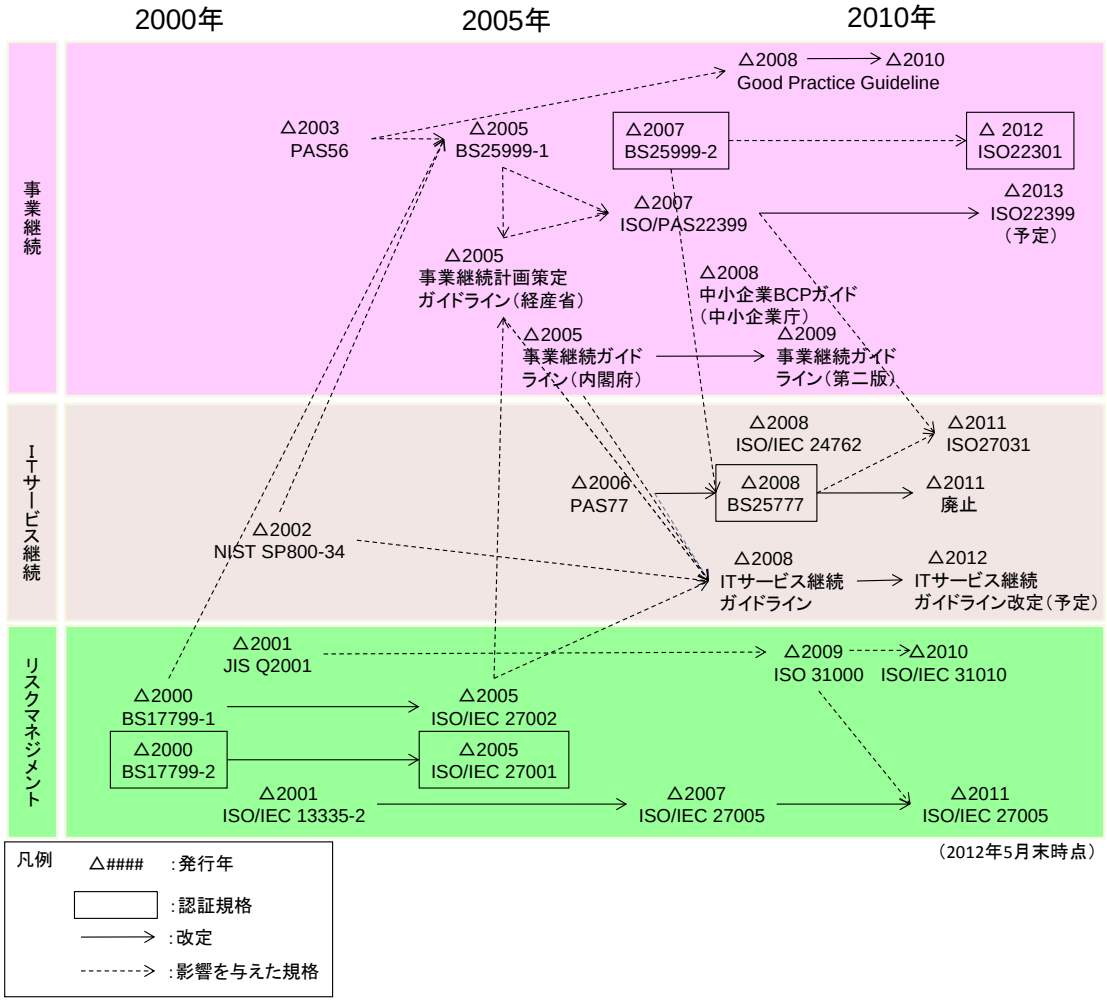


図 6-1 国際規格やガイドラインの関連図

なお、IPA が発行する「高回復力システム基盤導入ガイド」は、「IT サービス継続ガイドライン」（経済産業省）において示された IT サービス継続を確実にするための枠組み等を参考にしながら、事業継続戦略の策定やそれを実現する情報システム対策が十分にできていない企業や地方公共団体などが、「大規模災害」および「大規模システム」に備えた対応を容易に実施できるために策定されている。

6.2.3 国際規格およびガイドラインのプロフィール

6.2.2 で示した関連図の中から主要な国際規格およびガイドラインのプロフィールを示す。

(1) 事業継続（BCP/BCM）

① ISO 22301

項目	内容
名称	ISO 22301 Societal security –Business continuity management systems– Requirements※
発行年月	2012 年 5 月
発行主体	国際標準化機構（ISO:International Organization for Standardization） （英和対訳版:一般財団法人日本規格協会より発行予定（2012 年 5 月時点））
発行の目的等	事業継続マネジメントシステム（BCMS）の構築に関する要求事項を規定する。
備考	2012 年 5 月に国際規格として発行された。事業継続マネジメントシステムにおける要求事項が規定されている。 最終規格案（FDIS）の英和対訳版は日本規格協会より発行済みである。

※ 本規格を含め、以下に記載され日本規格協会が英和対訳版を発行している規格の原文および英和対訳版は、同協会（http://www.jsa.or.jp/）より入手可能である

② ISO/PAS 22399

項目	内容
名称	ISO/PAS22399 Social security –Guideline for incident preparedness and operational continuity management （社会セキュリティ ―緊急事態準備と業務継続マネジメントガイドライン）
発行年月	2007 年 12 月
発行主体	国際標準化機構（ISO:International Organization for Standardization） （英和対訳版:一般財団法人日本規格協会）

項目	内容
発行の目的等	組織における緊急事態準備と業務継続に関する理解、策定、導入のための基礎を提供し、組織と地域社会、事業と事業、そして組織と顧客/依頼人の取引に信用を提供する。
備考	ISO/PAS は ISO 一般公開仕様書(Publicly Available Specification)と言われ、公開から 3 年後に見直され、さらに 3 年間の期間延長がなされるか、国際規格とするために改正するか廃止するかが決定される。本規格は、2013 年までの国際規格化(ISO 化)に向け検討中である。

③ BS 25999-1

項目	内容
名称	BS 25999-1:2006 Business continuity management - Part1:Code of practice (事業継続マネジメント 第 1 部:実践規範)
発行年月	2006 年 11 月
発行主体	英国規格協会(BSI:British Standards Institution) (英和対訳版:一般財団法人日本規格協会)
発行の目的等	本規格は、事業継続マネジメントのプロセス・原則・用語を規定し、組織内で事業継続を理解し、構築し、実施するための基礎を提供し、企業間及び他組織との取引の信頼性を高めることを目的としている。
備考	本規格は、英国規格協会が 2003 年公表した「PAS56:2003 Guide to Business Continuity Management(事業継続管理のための指針)」の内容を継承している。 また、国際的に広く受け入れられており、ISO 22301 の内容にも影響を与えている。

④ BS 25999-2

項目	内容
名称	BS 25999-2:2007 Business continuity management - Part2:Specification (事業継続マネジメント 第 2 部:仕様)
発行年月	2007 年 11 月
発行主体	英国規格協会(BSI:British Standards Institution) (英和対訳版:一般財団法人日本規格協会)

項目	内容
発行の目的等	事業継続マネジメントを対象とするマネジメントシステムアプローチに対する要求事項を明確にするために作成された。組織の事業リスク全般の管理に対する考慮のもとで、文書化した BCMS（事業継続マネジメントシステム）を計画、確立、導入、運用、監視、レビュー、演習、維持及び改善するための要求事項について規定している。
備考	事業継続マネジメントシステムにおける認証規格である。

⑤ BCI Global Good Practice Guidelines 2010

項目	内容
名称	BCI Global Good Practice Guidelines 2010 Global Edition A Management Guide to Implementing Global Good Practice in Business Continuity Management（略称:GPG） （実践的ガイドライン 2010　グローバルエディション 事業継続マネジメント・グローバルを視点とした実践導入のためのマネジメントガイド）※
発行年月	2010 年 3 月
発行主体	The Business Continuity Institution（英国 BCI） （英和対訳版監修・翻訳:事業継続協会（BCI 日本支部）／出版:日本リスクマネジャー＆コンサルタント協会（RMCA Japan））
発行の目的等	BCM（事業継続マネジメント）の専門家及び個人の実務者の発展を支援する基盤及び共通の専門用語を提供する。BCM の学術機関や民間機関が活用できる、実績のある専門的なベンチマークを提供する。
備考	本版から、BS25999 への相互参照が無くなり、一部を除き BS25999 との直接的な相関を持たないことになったが、BS25999 との整合性は確保されている。

※ 英和対訳版は RMCA Japan の Web サイト（http://www.rmcaj.com/）より入手可能である

⑥ 事業継続ガイドライン

項目	内容
名称	事業継続ガイドライン　第二版 ― わが国企業の減災と災害対応の向上のために ―※
発行年月	2009 年 11 月（初版は 2005 年 8 月に発行）
発行主体	事業継続計画策定促進方策に関する検討会 内閣府 防災担当

項目	内容
発行の目的等	わが国企業に対して事業継続の取組みの概要および効果を示し、防災のための社会的な意義や取引における重要性の増大、自社の受けるメリット等を踏まえて企業が自主的に判断するのを促すものである。
備考	事業継続分野の ISO 規格では、適用範囲において汎用的なリスクを想定しているのに対して、本ガイドラインでは主として突発的に被害が発生するリスクのうち特に自然災害を想定している。

※ 内閣府防災担当の Web サイト(http://www.bousai.go.jp/kigyoubousai/jigyou/index.html)より入手可能である

⑦ 事業継続計画策定ガイドライン

項目	内容
名称	企業における情報セキュリティガバナンスのあり方に関する研究会報告書 参考資料　事業継続計画策定ガイドライン※
発行年月	2005 年 3 月
発行主体	経済産業省
発行の目的等	企業に対し BCP の概念自体の認知度向上を図りつつ、IT 事故発生時にも事業運営を継続的に維持するのに有効な BCP の普及に寄与すべく、IT 事故を想定した BCP の策定手順や検討項目等を解説する。
備考	企業における情報セキュリティガバナンスのあり方に関する研究会による報告書の中で、情報セキュリティガバナンスの確立を促進するための施策ツールの一つとして公開された。

※ 経済産業省の Web サイト(http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf)より入手可能である

⑧ 中小企業 BCP(事業継続計画)ガイド

項目	内容
名称	中小企業 BCP(事業継続計画)ガイド
発行年月	2008 年 3 月
発行主体	中小企業庁※
発行の目的等	本ガイドブックは、中小企業支援機関(地方自治体、商工会議所、商工会、中小企業団体中央会、政府系中小企業金融機関等)の関係者が、中小企業に BCP を説明し、BCP 策定について相談を受けた際に、概要や作成手法を簡単に説明するために活用する。

項目	内容
備考	中小企業庁では、中小企業にBCPを普及するため、「中小企業BCP策定運用指針（http://www.chusho.meti.go.jp/bcp/）」も併せて公開している。

※ 中小企業庁のWebサイト（http://www.chusho.meti.go.jp/keiei/antei/2008/080418bcp_gude.html）より入手可能である

(2) ITサービス継続（事業継続のための情報及び通信技術準備態勢）

① ISO/IEC 27031

項目	内容
名称	ISO/IEC27031 Information technology –Security techniques– Guidelines for information and communication technology readiness for business continuity （情報技術－セキュリティ技術－ 事業継続のための情報通信技術の準備態勢に関する指針）
発行年月	2011 年 3 月
発行主体	国際標準化機構（ISO：International Organization for Standardization） （英和対訳版:一般財団法人日本規格協会）
発行の目的等	事業継続のための情報通信技術（ICT）準備態勢の概念及び原則について記述し、事業継続を確実にするための、組織の ICT 準備態勢の改善に関するすべての側面（パフォーマンス基準、設計及び導入など）を特定して規定する方法及びプロセスの枠組みを提供する。
備考	ICT 準備態勢を、事業継続マネジメント及び情報セキュリティマネジメント（ISO/IEC 27001 に記述されている内容）の実施における不可欠の要素（それぞれの実施と運用の一部）と位置づけている。 また、事業継続のための ICT 準備態勢の計画及び実施に際し、ICT 災害復旧サービスの計画及び提供において、ISO/IEC 24762:2008 を参照することができるとしている。 ビジネスインパクト分析（BIA）で決定された継続の優先順位に従って、重要な活動を実施するための最低限の要求事項を定義し、ここから目標復旧時間（RTO）や目標復旧時点（RPO）を定めるとしている。付属書 A において詳細な設定の仕方が記載されている。

② ISO/IEC 24762

項目	内容
名称	ISO/IEC 24762 Information technology –Security techniques– Guidelines for information and communications technology disaster recovery services （情報技術－セキュリティ技法－情報及び通信技術障害復旧サービスの指針）
発行年月	2008 年 2 月
発行主体	国際標準化機構（ISO:International Organization for Standardization） 国際電気標準会議（IEC:International Electrotechnical Commission） （英和対訳版:一般財団法人日本規格協会）
発行の目的等	事業継続管理の一環としての情報通信技術災害復旧（ICT DR）サービスの提供に関する手引きを示して、情報セキュリティマネジメントシステム（ISMS）の運用を手助けすることを目的としている。
備考	技術的セキュリティ管理策は掲載しておらず、ISO/IEC 27001 及び ISO/IEC 27002 を含めた技術的な参考文献の参照を推奨している。付属書 A において ISO/IEC 27002：2005 とのセキュリティ管理策の対応を示している。

③ BS 25777

項目	内容
名称	BS 25777 Information and communications technology continuity management. Code of practice
発行年月	2008 年 11 月 （ISO/IEC 27031 の発行に伴い 2011 年 3 月に廃止）
発行主体	BSI:英国規格協会（British Standards Institution） （英和対訳版、邦訳版は発行されていない）
発行の目的等	IT サービス継続マネジメントの実践的な規範を示す。
備考	本規格は、英国規格協会が 2006 年公表した「PAS77 IT Service Continuity Management. Code of Practice（IT サービス継続マネジメント実践の規範）」の内容を継承している。 ISO/IEC 27031 が本規格の内容を継承し、2011 年 3 月に廃止されている。

④ IT サービス継続ガイドライン

項目	内容
名称	IT サービス継続ガイドライン※
発行年月	2008 年 9 月
発行主体	経済産業省
発行の目的等	組織における IT サービスの企画、開発、調達、導入、運用、保守などに携わる部門や担当者が、事業継続マネジメント(BCM)に必要な IT サービス継続を確実にするための枠組みと具体的な実施策を示し、取り組みの実効性の向上を支援することを目的とするものである。
備考	本ガイドラインでは、「ISO/IEC 20000(情報技術－サービスマネジメント－)はサービスレベル管理の基準であるが、本ガイドラインを用いることで IT サービス継続性というサービスレベル管理について ISO/IEC 20000 のマネジメントシステムを活用することができる」としている。

※ 経済産業省の Web サイト(http://www.meti.go.jp/policy/netsecurity/downloadfiles/itsc_gl.pdf)より入手可能である

⑤ SP800-34　IT システムにおける緊急時対応計画ガイド

項目	内容
名称	NIST Special Publication 800-34 Contingency Planning Guide for Information Technology (IT) Systems (IT システムのための緊急時対応計画ガイド)※
発行年月	2003 年 1 月
発行主体	米国国立標準技術研究所(NIST:National Institute of Standards and Technology) (翻訳文書:独立行政法人情報処理推進機構及び NRI セキュアテクノロジーズ株式会社)
発行の目的等	本ガイダンスでは、計画者が IT 要件を正確に反映し、緊急時対応計画原則を IT 運用のすべての側面に統合するコスト効率の高いソリューションを作成するのに役立つ体系的な方法を提供する。

※ 翻訳文書を独立行政法人情報処理推進機構(IPA)の Web サイト(http://www.ipa.go.jp/security/publications/nist/)より入手可能である

(3) リスクマネジメント

① ISO 31000

項目	内容
名称	ISO 31000 Risk management –Principles and guidelines （リスクマネジメント―原則及び指針）
発行年月	2009 年 11 月
発行主体	国際標準化機構（ISO:International Organization for Standardization） 国際電気標準会議（IEC:International Electrotechnical Commission） （英和対訳版:一般財団法人日本規格協会）
発行の目的等	リスクマネジメントに関する原則及び一般的な指針を示す。
備考	本規格は、「JIS Q 31000:2010 リスクマネジメント―原則及び指針」として 2010 年 9 月に JIS 化されている。

② IEC/ISO 31010

項目	内容
名称	IEC/ISO 31010 Risk management –Risk assessment techniques （リスクマネジメントーリスクアセスメント技法）
発行年月	2009 年 11 月
発行主体	国際標準化機構（ISO:International Organization for Standardization） 国際電気標準会議（IEC:International Electrotechnical Commission） （英和対訳版:一般財団法人日本規格協会）
発行の目的等	ISO 31000 の支援規格であり、リスクアセスメントのための体系的技法の選択及び適用に関する手引きを提供する。

③ ISO/IEC 27001

項目	内容
名称	ISO/IEC 27001 Information technology –Security techniques– Information security management systems – Requirements （情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項）
発行年月	2005 年 10 月

項目	内容
発行主体	国際標準化機構(ISO:International Organization for Standardization) 国際電気標準会議(IEC:International Electrotechnical Commission) (英和対訳版:一般財団法人日本規格協会)
発行の目的等	情報セキュリティマネジメントシステムを確立、導入、運用、監視、レビュー、維持及び改善するための要求事項を規定する。
備考	本規格は、2007 年 7 月に、情報セキュリティマネジメントシステムに関連する規格群を体系化する等のためにISO/IEC 17799-2 から規格番号が変更されている。 本規格は、「JIS Q27001:2006 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要求事項」として 2006 年 5 月に JIS 化されている。

④ ISO/IEC 27002

項目	内容
名称	ISO/IEC 27002 Information technology -Security techniques- Code of practice for information security management (情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範)
発行年月	2005 年 6 月
発行主体	国際標準化機構(ISO:International Organization for Standardization) 国際電気標準会議(IEC:International Electrotechnical Commission) (英和対訳版:一般財団法人日本規格協会)
発行の目的等	組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般原則について規定し、情報セキュリティマネジメントの共通に受容できる目標に関する一般的手引きを提供する。
備考	本規格は 2007 年 7 月に情報セキュリティマネジメントシステムに関連する規格群を体系化する等のため ISO/IEC 17799-1 から規格番号が変更されている。 本規格は、「JIS Q27002:2006 情報技術-セキュリティ技術-情報セキュリティマネジメントシステムの実践のための規範」として 2006 年 5 月に JIS 化されている。

⑤ ISO/IEC 27005

項目	内容
名称	ISO/IEC27005 Information technology –Security techniques– Information security risk management （情報技術–セキュリティ技術–情報セキュリティリスクマネジメント）
発行年月	2011 年 6 月（第 1 版は 2008 年 6 月に発行）
発行主体	国際標準化機構（ISO:International Organization for Standardization） 国際電気標準会議（IEC:International Electrotechnical Commission） （英和対訳版:一般財団法人日本規格協会）
発行の目的等	組織の情報セキュリティリスクマネジメントの指針、特に ISO/IEC 27001 に従った情報セキュリティマネジメントの要求事項を支援する。
備考	ICT セキュリティにおけるリスクマネジメントの手法が記載された規格である「ISO 13335-2」の考え方（特にリスクアセスメントに関する内容）が継承されている。

(4) その他（IT サービス管理）

① ISO/IEC 20000-1

項目	内容
名称	ISO/IEC 20000-1 Information technology –Service management– Part1:Service management system requirements （情報技術—サービスマネジメント— 第 1 部:サービスマネジメントシステム要求事項）
発行年月	2011 年 4 月（改定前の第 1 版は 2005 年 11 月に発行）
発行主体	国際標準化機構（ISO:International Organization for Standardization） 国際電気標準会議（IEC:International Electrotechnical Commission） （英和対訳版:一般財団法人日本規格協会）
発行の目的等	サービスマネジメントシステムを計画、確立、導入、運用、監視、レビュー、維持及び改善するための、サービス提供者に対する要求事項を規定する。

項目	内容
備考	本規格の第 1 版である「ISO/IEC 20000-1:2005」は、「JIS Q20001-1:2007 情報技術―サービスマネジメント―第 1 部:仕様」として 2007 年 4 月に JIS 化されている。 「IT サービス継続ガイドライン(経済産業省)」において、「IT サービス継続性というサービスレベル管理について ISO/IEC 20000 のマネジメントシステムを活用することができる」としている。

② ISO/IEC 20000-2

項目	内容
名称	ISO/IEC 20000-2 Information technology -Service management- Part2:Guidance on the application of service management systems (情報技術―サービスマネジメント― 第 2 部:サービスマネジメントシステムの適用の手引き)
発行年月	2012 年 2 月(第 1 版は 2005 年 12 月に発行)
発行主体	国際標準化機構(ISO:International Organization for Standardization) 国際電気標準会議(IEC:International Electrotechnical Commission) (英和対訳版:一般財団法人日本規格協会から発行予定(2012 年 5 月現在))
発行の目的等	本規格は、ISO/IEC20000-1 に基づいた、サービスマネジメントシステムの適用の手引きを示す。
備考	本規格の第 1 版である「ISO/IEC 20000-2:2005」は、「JIS Q20001-2:2007 情報技術―サービスマネジメント―第 2 部:実践のための規範」として 2007 年 4 月に JIS 化されている。 「IT サービス継続ガイドライン(経済産業省)」において、「IT サービス継続性というサービスレベル管理について ISO/IEC 20000 のマネジメントシステムを活用することができる」としている。

③ ITIL®

項目	内容
名称	ITIL® 2011 Edition
発行年月	2011 年 7 月
発行主体	英国政府内閣府(the Cabinet Office(旧 OGC))
発行の目的等	IT サービスマネジメントにおけるベストプラクティスを示す。

項目	内容
備考	ISO/IEC 20000 シリーズがサービスマネジメントにおける要求事項と適用の手引きを示すものとしているのに対して、ITIL®では IT サービスマネジメントのベストプラクティスを示すものとなっている。 ITIL® 2011 Edition は、ITIL® V3（2007 年 5 月発行）の update 版である。「サービスストラテジ」、「サービスデザイン」、「サービストランジション」、「サービスオペレーション」、「継続的サービス改善」の 5 つのコア書籍から構成される。 日本語書籍は ITIL® V3（itSMF Japan が主体となって翻訳作成※）が最新版である（2012 年 5 月時点）。 ITIL® is a Registered Trade Mark of the Cabinet Office.

※itSMF Japan の Web サイト（http://www.itsmf-japan.org/）より入手可能

以上