

# 情報システム基盤の復旧に 関する対策の調査

## 概要調査報告書

2012年7月

独立行政法人情報処理推進機構

- 
1. 調査全体の概要 ……2ページ
  2. 文献調査 ……4ページ
  3. アンケート調査 ……12ページ
  4. ヒアリング調査 ……18ページ
  5. 考察 – 企業等の情報システム基盤の復旧能力の向上に向けて – ……22ページ

# 1. 調査全体の概要

## 1.1 目的と方法

### 目的

本調査は、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、企業等の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として行った。

このために、東日本大震災発生時の被災企業の対応事例や、復旧にあたり利用された仮想化やクラウド等の新しい技術やサービスの事例、民間企業等におけるデータの保管対象や方法等を調査し、調査結果は報告書として取りまとめるとともに、『高回復カシステム基盤導入ガイド』の内容との対比を行った。

### 文献調査

報告書、専門書籍、雑誌、Web資料等を対象に調査を実施

- ①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、被災前後における企業の対策状況と意識の変化
- ②システム復旧に関連する新しい技術やサービス

### 文献調査(付録)

事業継続、ITサービス継続、リスクマネジメント等に関する主要な国際規格やガイドラインを調査

### アンケート調査

企業3,000社に対して調査を実施

- 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

### ヒアリング調査

企業・地方公共団体11組織を対象に調査を実施

- 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

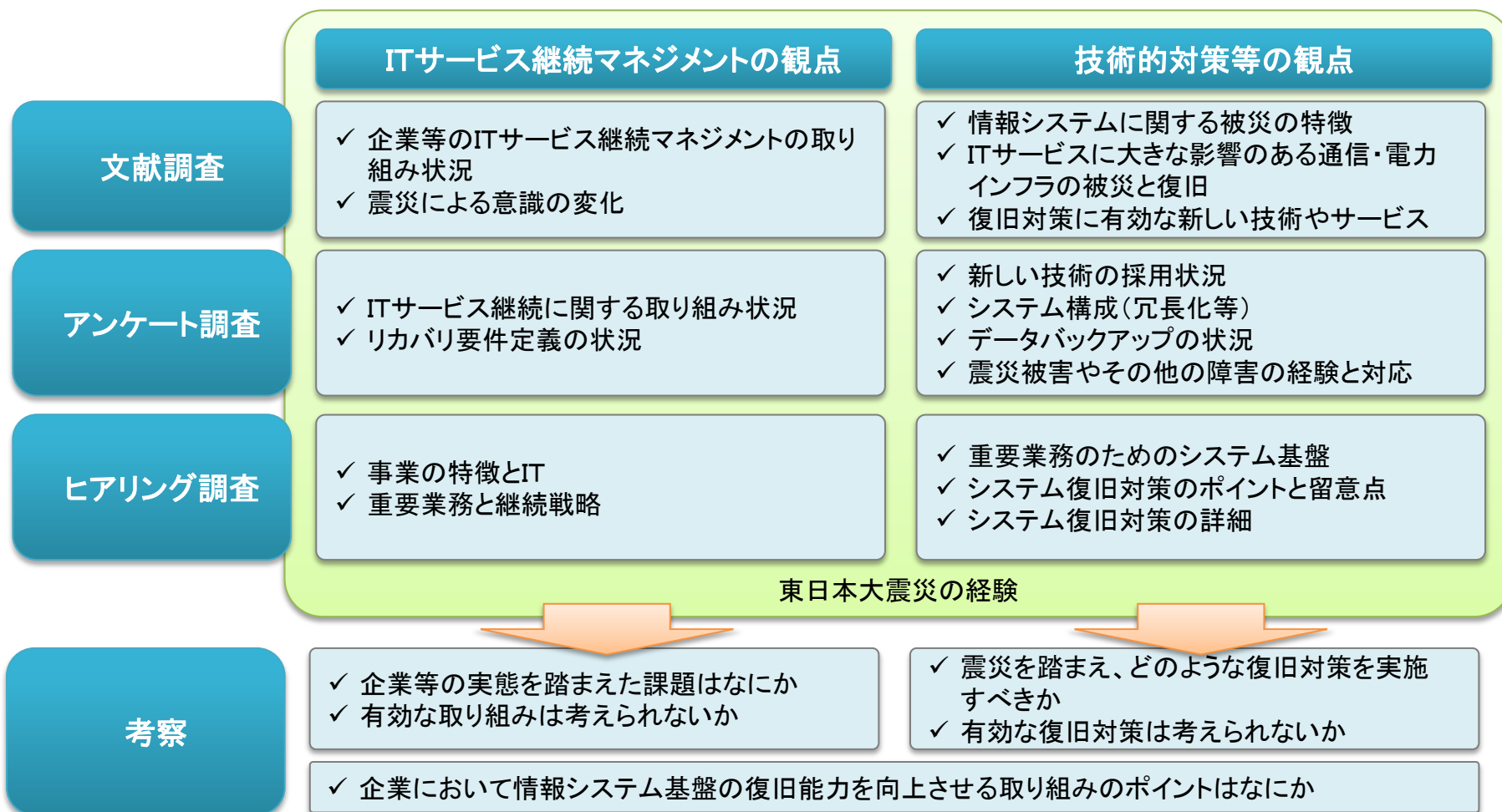
### 考察・ガイドとの比較

- ITサービス継続マネジメントの観点
- 情報技術的対策等の観点

- 概要編との対比(4つのモデルの採用状況、主要要件)
- 計画編との対比(4つのモデルの要件、対策例)

## 1.2 調査の注視点

- 東日本大震災の経験を活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」、「技術的対策等の観点」の2つの観点到に注視して、情報システム基盤の復旧対策について調査を実施した。



# 2. 文献調査

## 2.1 文献調査の概要

項目	内容		
調査対象	調査項目	対象資料	収集資料数
	(1) 企業等のITサービス継続戦略に関する意識と変化 (2) 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	○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	○文献:10種類 ○記事・Web資料:20種類
	(3) ITサービスに関連する社会インフラの被災と復旧	○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	○文献:5種類 ○記事・Web資料:5種類
	(4) 新しい技術・サービスの活用	○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	○文献:10種類 ○記事・Web資料:15種類
調査期間	2012年3月～4月		

## 2.2 文献調査結果の総括 [1/2]

分類	調査結果概要	着目した理由
(1)企業等のITサービス継続戦略に関する意識と変化	<ul style="list-style-type: none"> <li>・震災を受け、システムの災害対策の見直しの機運は高まり、BCP(事業継続計画)の認知も進んでいる。しかし、BCPを策定している企業は少ない。</li> <li>・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ができていない企業では、BCPが十分に機能していない。</li> <li>・震災では、事前の想定を超える事態が発生した。システム設置拠点の損壊や、被害の広域化、長期化等は想定を超えていた。</li> </ul>	<ul style="list-style-type: none"> <li>・事業継続の取り組みに重要と言われるBCPを策定している企業は少ない、という実態を前提に、有効な復旧対策を検討する必要があると考えたため。</li> <li>・事業継続において、重要業務・サービスの設定や目標復旧時間の設定は、優先的に取り組むべき事項であると考えたため。</li> <li>・震災の経験から、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であると考えたため。</li> </ul>
(2)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	<ul style="list-style-type: none"> <li>・復旧手順の確立、データバックアップ、通信・電力確保が重要と考える企業が多い。</li> <li>・BCP策定済み企業においても、教育訓練や維持改善等の取り組みが実行できていない。</li> </ul>	<ul style="list-style-type: none"> <li>・企業が課題として認識している復旧手順の確立、データバックアップ、通信・電力確保に留意した復旧対策を検討する必要があると考えたため。</li> <li>・BCP策定済み企業においても事業継続マネジメントの取り組みが十分でない実態を踏まえ、有効な復旧対策を検討する必要があると考えたため。</li> </ul>

## 2.2 文献調査結果の総括 [2/2]

分類	調査結果概要	着目した理由
(3)ITサービスに関連する社会インフラの被災と復旧	<ul style="list-style-type: none"> <li>・通信・電力とも、サービスの停止が、広域的、長期的に発生した。</li> <li>・震災後も計画停電により、電力供給が一時的に中断する事象も発生した。</li> </ul>	<ul style="list-style-type: none"> <li>・通信、電力のサービス停止が広域的、長期的に発生する前提で対策を検討する必要があることが明らかとなったため。</li> </ul>
(4)新しい技術・サービスの活用	<ul style="list-style-type: none"> <li>・サーバ仮想化環境においては、信頼性向上・バックアップサイト構築に関わる技術が充実しつつあり、従来の技術(二重化、クラスタリング)よりも効率的に復旧能力の高いシステム基盤を構築できる。</li> <li>・ただし、仮想化技術の利用にあたってはソフトウェアの動作保障・動作確認や、ライセンス費用等で留意が必要。</li> </ul>	<ul style="list-style-type: none"> <li>・留意点を踏まえた上で、サーバ仮想化技術やクラウドサービスを活用することは、有効な復旧対策となり得ることを示すため。</li> </ul>
(付録)関連する国際規格・ガイドラインの関係	<ul style="list-style-type: none"> <li>・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およびそれらの関連性を調査。</li> </ul>	

## 2.3 文献調査の結果

### (1) 企業等のITサービス継続戦略に関する意識と変化

#### 【調査の概要】

震災後の企業等の経営に対するITサービス継続に対する意識や対象とするリスクのへの認識の変化等を調査。

項目	概要	参考文献資料
業務の IT依存度分析	<ul style="list-style-type: none"> <li>企業の今後3年間の経営課題として震災前の時点で順位の低かった「災害対策やシステムダウンへの対応(BCP/DR)」が、震災後第1位に挙げられている。</li> <li>震災後、8割を超える企業がシステム環境の災害対策を見直す必要があると考えている。</li> </ul>	JIPDEC「企業IT利活用動向調査」 日経BP社「ITで実現する震災・省電力BCP完全ガイド」
	<ul style="list-style-type: none"> <li>震災を受けBCPの認知は高まっているものの、策定済み企業数は少ない(大企業で30.9%、中小企業では8.6%)。</li> </ul>	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」
ITサービス継続 の要件定義	<ul style="list-style-type: none"> <li>BCPを策定している多くの企業が重要な業務・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を実施している。これらを実施していない企業では、BCPが十分に機能していない割合が高い。</li> </ul>	野村総合研究所「震災後のBCP(事業継続計画)に関するアンケート」
リスク評価	<ul style="list-style-type: none"> <li>震災被害の特徴               <ul style="list-style-type: none"> <li>-津波による拠点施設の損壊や原子力災害の発生等の想定外の被害が発生した。</li> <li>-被害が広域化、長期化し、直接被害だけでなく、間接被害が多く発生した(電力、通信等)。</li> </ul> </li> <li>被災企業のうち、ITシステム、通信、電力の供給について、9割の企業が復旧するまでに2週間程度を要した(9割にはこれらの被害のなかった企業を含む)。</li> </ul>	ISN「東日本大震災と自治体ICT公開セミナー」資料、東京海上日動リスクコンサルティング「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」他
	<ul style="list-style-type: none"> <li>震災後、広域災害について多く認識されるようになった。また、原子力災害についても注目が集まった。</li> </ul>	NTTデータ経営研究所「東日本大震災を受けた企業の事業継続に係る意識調査」
	<ul style="list-style-type: none"> <li>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。</li> </ul>	JUAS「企業IT動向調査2012」



## (2) 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

### 【調査の概要】

震災後の企業等がITサービス継続のために採用した対策や取り組み、意識の変化等を調査。

項目	概要	参考文献資料
対策実施計画	<ul style="list-style-type: none"> <li>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、遠隔地のシステムによるバックアップを指摘する企業が多い。</li> </ul>	日経BP社『ITで実現する震災・省電力BCP完全ガイド』
	<ul style="list-style-type: none"> <li>震災後、クラウドの利用を検討している企業は比較的多い。</li> </ul>	JUAS「企業IT動向調査2012」
	<ul style="list-style-type: none"> <li>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、データバックアップの必要性を指摘する比率が高い。</li> </ul>	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」
	<ul style="list-style-type: none"> <li>基幹システムのデータバックアップを行っている企業は8割強であり、震災以降、未実施の企業のうち過半数が、データバックアップを実施する意向を持っている。</li> <li>震災以前に基幹システムのデータバックアップを行っていた企業の約6割が、同一のビル・建物を保管場所としている。震災後、遠隔地バックアップの意向を持つ企業は多い。</li> </ul>	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』
教育訓練計画	<ul style="list-style-type: none"> <li>BCP/BCM全般について、社内教育や訓練を実施していない企業は6割以上。</li> </ul>	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」
事後対応計画 (緊急時対応計画)	<ul style="list-style-type: none"> <li>バックアップからの復旧手順は半数以上の企業で震災以前から整備されていた。</li> <li>震災時、手順どおり復旧できたという企業が多いものの、改善の余地を残す企業も一定数存在する。</li> </ul>	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』
維持改善計画	<ul style="list-style-type: none"> <li>BCM全般について、定期的に見直す仕組みや評価する指針を有していない企業は6割以上。</li> </ul>	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」

### (3) ITサービスに関連する社会インフラの被災と復旧

#### 【調査の概要】

ITサービス継続に影響を与える通信、電力についての東日本大震災時の被災と復旧状況を調査。

項目		概要	参考文献資料
通信	固定通信網	<ul style="list-style-type: none"> <li>・NTT東日本・KDDI・ソフトバンクテレコムで約190万回線が被災。NTT東日本では、385の通信ビルが機能停止。固定電話では影響回線数が半減するのに2～3日を要した。4月末までに一部地域を除き復旧。</li> <li>・NTT東日本では、震災直後、通常の4～9倍のトラフィックが発生。最大80～90%発信規制を実施。東北地方だけでなく首都圏等でも通話に支障。</li> </ul>	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」
	携帯電話(PHS含む)	<ul style="list-style-type: none"> <li>・基地局については、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で最大約29,000局が停波。停波基地局数が半減するのに2～3日を要した。4月末までに一部地域を除き復旧。</li> </ul>	
		<ul style="list-style-type: none"> <li>・音声では、震災直後、通常の50～60倍のトラフィックが発生(NTTドコモ)。最大70～95%の発信規制を実施。東北地方だけでなく首都圏等でも通話に支障。</li> <li>・パケットについては、音声ほどのトラフィックは発生しなかった。発信規制はNTTドコモのみが実施(最大30%)。</li> </ul>	
電力	<ul style="list-style-type: none"> <li>・震災直後、東北電力管内において約466万戸の停電が発生。停電戸数半減するのに1～2日を要した。震災発生1か月後には、一部地域を除き復旧。</li> <li>・同様に、東京電力管内において約405万戸の停電が発生。3月19日までにはすべて復旧したが、3月14日から28日の間の計10日間、延べ32回、計画停電が実施された。</li> </ul>	岐阜大学教授能島暢呂「東日本大震災におけるライフライン復旧概況(時系列編)」、経済産業省資料	

## (4) 新しい技術・サービスの活用 ①技術(サーバ仮想化等)

### 【調査の概要】

システム復旧対策に有用と考えられる、サーバ仮想化技術を調査(2012年4月時点)。

適用箇所	とりあげた技術	概要
同一サイト内 信頼性向上	高可用性機能	<ul style="list-style-type: none"> <li>・サーバ仮想化環境におけるサーバ二重化・クラスタリングに相当する機能。</li> <li>・既存の技術よりも比較的容易に動作環境が整備できる。</li> </ul>
バックアップ サイト構築	災害対策機能	<ul style="list-style-type: none"> <li>・サーバ仮想化環境におけるバックアップサイトの構築支援機能。</li> <li>・従来の技術よりも比較的容易にバックアップサイトが構築できる。</li> </ul>
	重複排除機能	<ul style="list-style-type: none"> <li>・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ひとつにまとめる機能。</li> <li>・バックアップデータ容量が減少するため、バックアップメディア容量の縮小と、遠隔バックアップ高速化の効果がある。</li> </ul>
	バックアップ アプライアンス	<ul style="list-style-type: none"> <li>・バックアップ専用装置だが、ソフトウェアが動作する環境もあり、業務継続に利用できる。</li> <li>・小規模であれば安価にバックアップサイトが構築できる。</li> </ul>

## (4) 新しい技術・サービスの活用 ②サービス(クラウドサービス等)

### 【調査の概要】

システム復旧対策に有用と考えられる、クラウドサービスを調査(2012年4月時点)。

適用箇所	とりあげたサービス	概要
バックアップの 遠隔地保管	遠隔バックアップサービス	<ul style="list-style-type: none"> <li>・遠隔バックアップサービスには専用型、共用型、ストレージベンダ限定型がある。</li> <li>・堅牢なデータセンタにバックアップを保管できる効果に加え、バックアップに関わる管理・運用負荷を軽減する効果がある。</li> <li>・データ量によっては、ネットワークがボトルネックになることによるバックアップの長時間化、あるいは利用料金が増大することがある。</li> </ul>
	データセンタ／クラウドの 付加サービス	<ul style="list-style-type: none"> <li>・データセンタ／クラウドサービスの付加サービスとして、バックアップサービスが利用できる場合がある。</li> <li>・上記以外に、複数データセンタにデータを保管するサービスもある。</li> <li>・すべてのデータセンタ／クラウドサービスで利用できるわけではないので、利用にあたり確認が必要である。</li> </ul>
バックアップ サイト構築	IaaS等	<ul style="list-style-type: none"> <li>・IaaS等のクラウドサービスを利用することで、バックアップサイトを構築することができる。</li> </ul>

# 3. アンケート調査

## 3.1 アンケート調査の概要

項目	概要
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から任意に抽出した3,000社
調査依頼先	情報システム部門の責任者(ITサービス継続や情報システム基盤の復旧対策(データの保管等)に関わると思われるため)
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%)

### (参考)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を母集団としている。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。



## 3.2 アンケート調査結果の総括

分類	調査項目	調査結果概要	着目した理由
①ITサービス継続に関する取り組み状況	<ul style="list-style-type: none"> <li>BCPやIT-BCP(情報システム部門におけるBCP)の策定状況</li> <li>ITサービス継続に関する活動の状況</li> <li>想定したリスクや重点的に取り組んでいる領域</li> </ul>	<ul style="list-style-type: none"> <li>IT-BCP策定企業は1/4にとどまる。</li> <li>IT-BCP策定企業であってもITサービス継続マネジメントプロセスに満遍なく取り組めていない。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>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おらず、今後の課題であることを示すとともに、その実態を踏まえた対策が必要であると考えたため。</li> </ul>
②コンピュータシステムと新しい技術の採用状況	<ul style="list-style-type: none"> <li>利用しているシステムとバックアップ対象の確認</li> <li>仮想化やクラウドの利用状況</li> </ul>	<ul style="list-style-type: none"> <li>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である。</li> <li>仮想化導入とクラウドの利用には正の相関がある。</li> </ul>	<ul style="list-style-type: none"> <li>クラウドサービスは復旧対策に有効であるとの企業の評価を示すため。</li> </ul>
③システム構成	<ul style="list-style-type: none"> <li>システムの冗長化の確認</li> </ul>	<ul style="list-style-type: none"> <li>事業規模やIT依存度が大きいほど対策が充実。</li> <li>待機系システムが設置されている企業は約半数、遠隔地に設置している企業は15%にとどまる。</li> </ul>	<ul style="list-style-type: none"> <li>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の必要性を示すため。</li> </ul>
④リカバリ要件定義の有無	<ul style="list-style-type: none"> <li>目標復旧時間(RTO)、目標復旧レベル(RLO)、目標復旧時点(RPO)の設定状況</li> </ul>	<ul style="list-style-type: none"> <li>RTOを設定している企業は2割程度にとどまる。</li> <li>取り組みが進んでいる企業はRTOを設定している。</li> <li>戦略(RTO)と対策間で不整合が見られる。</li> </ul>	<ul style="list-style-type: none"> <li>RTO設定企業が少ないという課題に加え復旧対策に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ことを示すため。</li> </ul>
⑤データの保管(バックアップ)の状況	<ul style="list-style-type: none"> <li>バックアップポリシーの整備状況</li> <li>バックアップの実施状況</li> </ul>	<ul style="list-style-type: none"> <li>事業規模やIT依存度が大きいほど対策が充実。</li> <li>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にとどまる。</li> </ul>	<ul style="list-style-type: none"> <li>IT依存度に応じたデータ保管対策の実施が重要であることを示すため。</li> </ul>
⑥震災被害やその他の障害の経験とその後の対応	<ul style="list-style-type: none"> <li>被災後に不十分だと感じた対策</li> <li>過去に復旧に失敗した事例</li> </ul>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>復旧対策において、データの保管方法の見直しが注目されていることを踏まえた対策が必要であると考えたため。</li> <li>電力やインフラ等のインフラ面への対策が重要であることを示すため。</li> </ul>

(文献調査との対比)

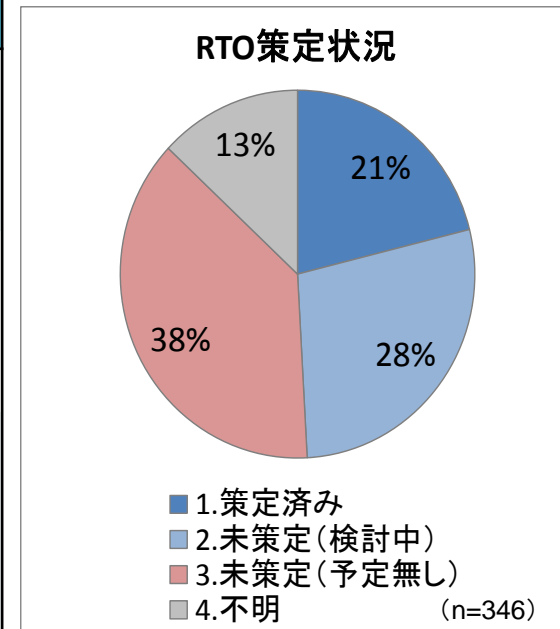
- BCPの認知は高まっているものの策定している企業は少ないという、文献調査と同様の傾向がみられた。
- 文献調査では、対策全般への意向として「災害発生時のシステム復旧手順」や「別拠点への重要データのバックアップ」が上位に挙げられていたり、バックアップに関する意欲の変化に「遠隔バックアップの実施を開始したい」とする企業が48.3%あったが、アンケート調査でもそれらの傾向と同様の結果が得られている。

## 3.3 アンケート調査の結果 [1/4]

<b>①ITサービス継続に対する意識や平常時の準備や活動</b> <b>【調査の概要】 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を調査。</b>	<b>設問</b>
<ul style="list-style-type: none"> <li>・BCP策定済みは40%、未策定(検討中)は33%。IT-BCP策定済みは25%、未策定(検討中)は41%。</li> <li>・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。</li> </ul>	Q9,Q10
<ul style="list-style-type: none"> <li>・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%。一方、BIA(ビジネスインパクト分析)の実施(25%)やRTO等の策定(28%)、教育訓練計画策定(19%)、事後対策計画策定(30%)、維持改善計画(17%)と、ITサービスの特定以外の割合は相対的に低い。文書の作成だけでなく、十分な戦略の策定や教育訓練、継続的な見直しが重要。</li> </ul>	Q11
<ul style="list-style-type: none"> <li>・ITサービス継続策定時に想定するリスクは、上位から地震、ハードウェア故障と停電が同数、次いで通信回線関連の故障、建物や施設の損壊の順となっている。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。</li> </ul>	Q6,Q12
<ul style="list-style-type: none"> <li>・重点的に取り組んでいる領域は、上位から電源・ネットワークの冗長化、データの遠隔地保管、機器等の冗長化の順となっている。</li> </ul>	Q13
<b>②コンピュータシステムと新しい技術の採用状況</b> <b>【調査の概要】 重要な情報システムを特定し、新しい技術の採用状況を調査。</b>	<b>設問</b>
<ul style="list-style-type: none"> <li>・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・給与システムが多い。業種毎で見ると、製造業で生産管理システムを多く挙げられるなど、業種の特徴により重要システムが異なる傾向がある。</li> </ul>	Q16 ※3
<ul style="list-style-type: none"> <li>・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。</li> </ul>	Q16,Q17
<ul style="list-style-type: none"> <li>・仮想化とクラウドの利用には相関がある(仮想化利用のクラウド利用は54%、仮想化未利用のクラウド利用は21%)。</li> </ul>	Q18,Q20
<ul style="list-style-type: none"> <li>・クラウド導入を検討している企業の導入目的として、災害対策が筆頭にあげられている</li> <li>・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伺える(利用中企業:運用費低減&gt;導入費低減&gt;災害対策、検討中企業:災害対策&gt;運用費低減&gt;導入費低減)。</li> </ul>	Q20,Q21

## 3.3 アンケート調査の結果 [2/4]

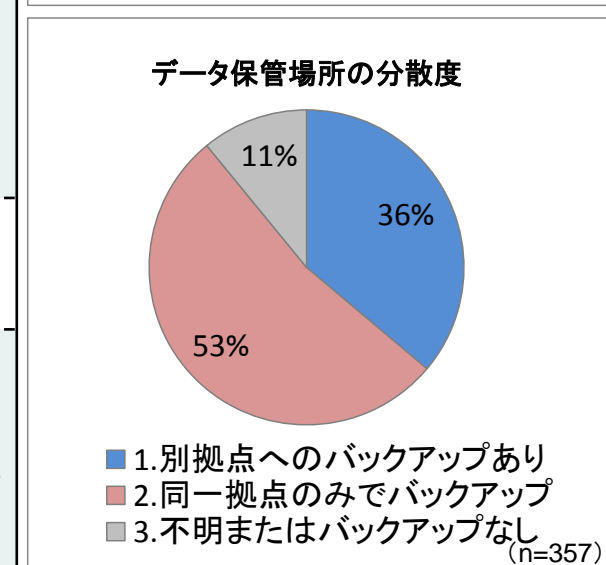
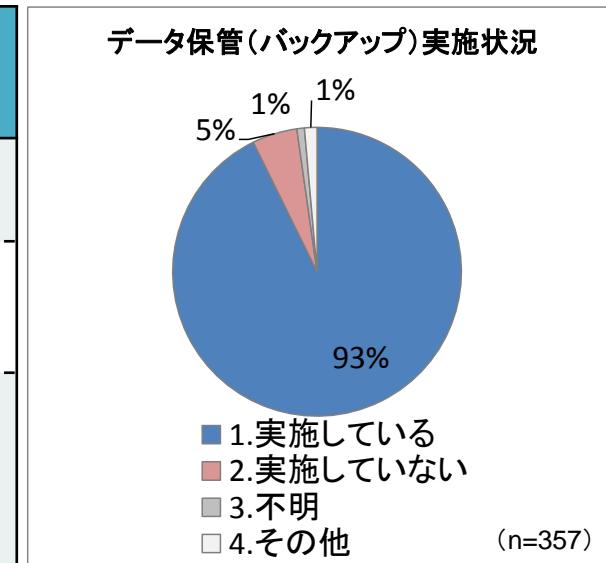
③システム構成 【調査の概要】 システム構成や冗長化の状況を調査。	設問
・待機系システムを設置している企業は全体の53%、遠隔地にも待機系システムを設置しているのは15%。	Q23
・資本金の額、拠点数、従業員数、IT依存度の高さに応じて、システムを冗長化している傾向が強い。	Q6,Q23
・同一サイトでの復旧作業を一部でも自動化している企業は45%、遠隔地のバックアップサイトでは21%となっており、バックアップサイトでの作業は自動化せずに手作業で実施する割合が高い。	Q25
④リカバリ要件定義の有無 【調査の概要】 サービス継続の復旧目標の設定状況を調査。	設問
・RTOを策定している企業は約2割(右のグラフ参照)。RLO、RPOでも同様の傾向である。BCP、IT-BCPを策定している企業ほど設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。	Q9,Q10, Q26,Q27, Q28
・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、RTOを策定済みとしている企業の割合が多い。ITサービス継続の取り組みにおいて、複数部門を巻き込んでいく上で、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。	Q11,Q26
<ul style="list-style-type: none"> <li>・RTOの設定時間で最も多いのは、「1～6時間」。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」。RPOで最も多いのは、「障害・被災発生の前日まで復旧」。</li> <li>・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との整合性を確保することが重要である。</li> </ul>	Q26,Q27, Q28





# 3.3 アンケート調査の結果 [3/4]

⑤データの保管(バックアップ)の実施状況 【調査の概要】 データ保管(バックアップ)の実施状況を調査。	設問
・データの保管(バックアップ)を実施している企業は、93%(右上段のグラフ参照)。	Q29
・バックアップポリシーを全部又は一部のシステムで明確化している企業は71%。	Q30
<p>・バックアップポリシーを明確化していない26%の企業のうち、59%は事業のIT依存度が高いとしている。</p> <p>・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、適切な復旧目標を策定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。</p>	Q8,Q30
・バックアップデータは36%が別拠点に保管しており、53%がシステム設置拠点と同一の拠点のみに保管(右下段のグラフ参照)。	Q38
・データの保管対策は、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。	Q2,Q8, Q29~42



## 3.3 アンケート調査の結果 [4/4]

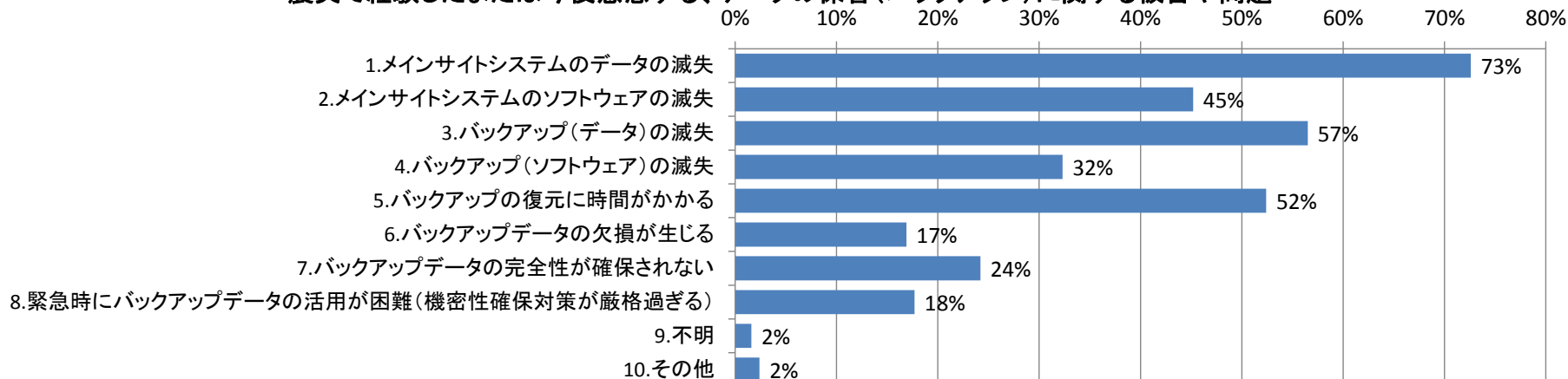
### ⑥ 震災被害やその他の障害の経験とその後の対応

【調査の概要】 復旧対策の有効性を調査。

設問

- |  |     |
|--|-----|
| ・情報システムの利用を制限された経験のある震災は、東日本大震災が最も多い。  | Q43 |
| ・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が36%。対策の検討に至らなかったのは28%。震災前の対策で十分だと認識し現状維持とした企業は25%。                               | Q44 |
| ・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。   |     |
| ・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として、メインサイトシステムのデータ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を要する、が上位に挙げられている(下記のグラフ参照)。 | Q45 |
| ・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、データの保管場所の見直し、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。              | Q46 |
| ・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いる。             | Q47 |

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)

# 4. ヒアリング調査

## 4.1 ヒアリング調査の概要

項目	内容				
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				
	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	<ul style="list-style-type: none"> <li>サーバ仮想化技術採用し、海外にバックアップサイトを設置。</li> <li>同期バックアップを行い、震災時にフェイルオーバーを実施。</li> </ul>
		B社	決済代行システム	サービス業	<ul style="list-style-type: none"> <li>障害対策のため、メインサイトの冗長化や回線の三重化を実施。</li> </ul>
		C社	Webサービス(情報提供)、プログラマーを管理するプライベートSNS	サービス業	<ul style="list-style-type: none"> <li>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。</li> </ul>
		D社	売買システム	金融・保険業	<ul style="list-style-type: none"> <li>システム障害対策のため、メインサイトは三重化を実施。</li> </ul>
	外部向け窓口システム	E団体	住民基幹系情報システム(住民記録・税・福祉)	地方公共団体	<ul style="list-style-type: none"> <li>東日本大震災時に庁舎が津波により被災。</li> <li>遠隔地のバックアップデータで一部のデータを復旧。</li> </ul>
	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	<ul style="list-style-type: none"> <li>水害によりサーバの水没の経験。</li> <li>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。</li> </ul>
		G社	生産管理システム、顧客管理システム、財務・会計管理システム、メール・グループウェア等	製造業	<ul style="list-style-type: none"> <li>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耐火金庫内に保管。</li> </ul>
		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	<ul style="list-style-type: none"> <li>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。</li> </ul>
		I社	ERP、メール・グループウェアシステム	サービス業	<ul style="list-style-type: none"> <li>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。</li> <li>クラウドサービスも活用。</li> </ul>
		J社	契約者情報管理システム	その他	<ul style="list-style-type: none"> <li>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。</li> </ul>
		K団体	IT基盤システム(全庁ネットワーク、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	<ul style="list-style-type: none"> <li>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。</li> <li>住民基幹系システムは遠隔地バックアップを実施。</li> </ul>
調査時期	2012年4月～5月				

## 4.2 ヒアリング調査結果の総括

項目	概要	着目した理由
①事業の特徴とIT	<ul style="list-style-type: none"> <li>IT-BCPの策定やBIAを実施している企業等は少ない。作業負担やノウハウ不足が理由。</li> </ul>	<ul style="list-style-type: none"> <li>ITサービス継続において、IT-BCPの策定やBIAの実施が望ましいが企業にとって容易ではなく、その実態を踏まえた有効な対策を検討する必要があるため。</li> </ul>
②重要業務と継続戦略	<ul style="list-style-type: none"> <li>事例では、BIA未実施でも利益・売上高や顧客サービスへの影響、業界の規定、災害時対応の緊急性等から重要業務を定めている。</li> <li>事例では、BIA未実施でも、業界の規定、顧客とのSLA、経験値、実現性、コスト等から復旧目標を定めている。</li> </ul>	<ul style="list-style-type: none"> <li>BIAを実施しないで、重要業務や復旧目標(ITサービス継続戦略の重要な要素)を設定する、実践的な知見と考えたため。</li> </ul>
③重要業務のためのシステム基盤の概要	<ul style="list-style-type: none"> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>システム構成の決定方法の実践的な知見と考えたため。</li> </ul>
④システム復旧対策のポイントと留意点	<ul style="list-style-type: none"> <li>被災経験からは、人、データ、通信・電力、建物等の資源全般が喪失することへの備えが必要との教訓。</li> <li>リスクを特定するのではなく、システムに関連する資源の状態に基づき対策の発動を決定する例がある。</li> <li>仮想化技術によりサーバを統合化し、コスト増を抑えてバックアップサイトを構築している例がある。</li> </ul>	<ul style="list-style-type: none"> <li>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の重要性の指摘と対策例の知見が得られたため。</li> <li>新しい技術の有効な活用例と考えたため。</li> </ul>
⑤システム復旧対策の詳細	<ul style="list-style-type: none"> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>データの保全、遠隔地バックアップの重要性を示す知見と考えたため。</li> </ul>

## 4.3 ヒアリング調査の結果 [1/2]

### ①事業の特徴とIT

【調査の概要】 企業のITの活用状況やITガバナンスの取り組みを調査。

- ・対象企業等はIT依存度が高いと認識している企業が多い。
- ・IT-BCPを策定している企業は少ない。
- ・BIAを実施している企業等は少ない。作業負担やノウハウ不足が実施していない理由となっている。
- ・システムの復旧対策は、情報システム部門が中心となって検討しており、それぞれ根拠となる考えや尺度を持っている。

### ②重要業務と継続戦略

【調査の概要】 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。

- ・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。
- ・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、コスト等から定めている。
- ・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。

### ③重要業務のためのシステム基盤の概要

【調査の概要】 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。

- ・事例では、認識しているリスクに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システム構成を決定している。

## 4.3 ヒアリング調査の結果 [2/2]

### ④システム復旧対策のポイントと留意点

【調査の概要】 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。

- ・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。
- ・リスクを特定するのではなく、システムに関連する資源の状態に基づき対策の発動を決定する例がある(資源に着目した対策を実施)。
- ・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例、遠隔地のバックアップサイトに切り替えた例があった。
- ・仮想化技術を導入し、サーバ統合化を進めながら、コスト増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理由から仮想化を導入していない場合もある。

### ⑤システム復旧対策の詳細

【調査の概要】 情報システム基盤の復旧対策の詳細を調査。

- ・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。
- ・大規模災害時においても短時間で復旧を目指す企業においては、遠隔地に待機系システムを設置し、短い間隔でバックアップを実施している。
- ・非常時の通信確保に、衛星インターネットあるいは建物間通信に無線LANの技術を活用した例等、無線技術の活用が有効に機能した例があった。

# 5. 考察 –企業等の情報システム基盤の復旧能力の向上に向けて–

## 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

#### 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、策定済み企業数は少ない
- ✓ 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、維持改善計画

### 技術的対策等の観点

- ✓ 企業はデータバックアップ、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を策定している企業、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

## 5.2 ITサービス継続マネジメントの観点

### ITサービス継続マネジメントの確立と定着

- ・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、マネジメントシステムを確立していくことが望まれる。震災後、企業等の意識は高まっており、普及・啓発の好機となっている。
- ・調査結果からは、「BIA」、「教育訓練」、「維持改善」等が実施されている例は少なく、ITサービス継続マネジメントシステムを確立している企業等は少数である(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認識されていないと推察)。
- ・調査結果から、企業等にとってBIA等の実施は容易ではないことが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と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。

### 重要業務と復旧目標の明確化

- ・ヒアリング調査結果からは、BIAの実施やIT-BCPの策定を行っていない企業でも、それぞれの考え方や尺度を持ち、有効性が高いと考えられるシステム復旧対策を実施している。
- ・その場合、重要業務、復旧目標については組織として検討・決定し、対策を実施している例が多い。
- ・アンケート調査結果からは、RTOを設定している企業は、ITサービス継続の各取り組みを広範に実施している傾向があり、目標・指標設定を行うことは復旧対策の推進に有効と考えられる。
- ・まずは、ITサービス継続の基本的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重要と考える。



## 5.3 技術的対策等の観点

- 東日本大震災の被災経験を踏まえると、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、それを代替する対策が重要と考える。

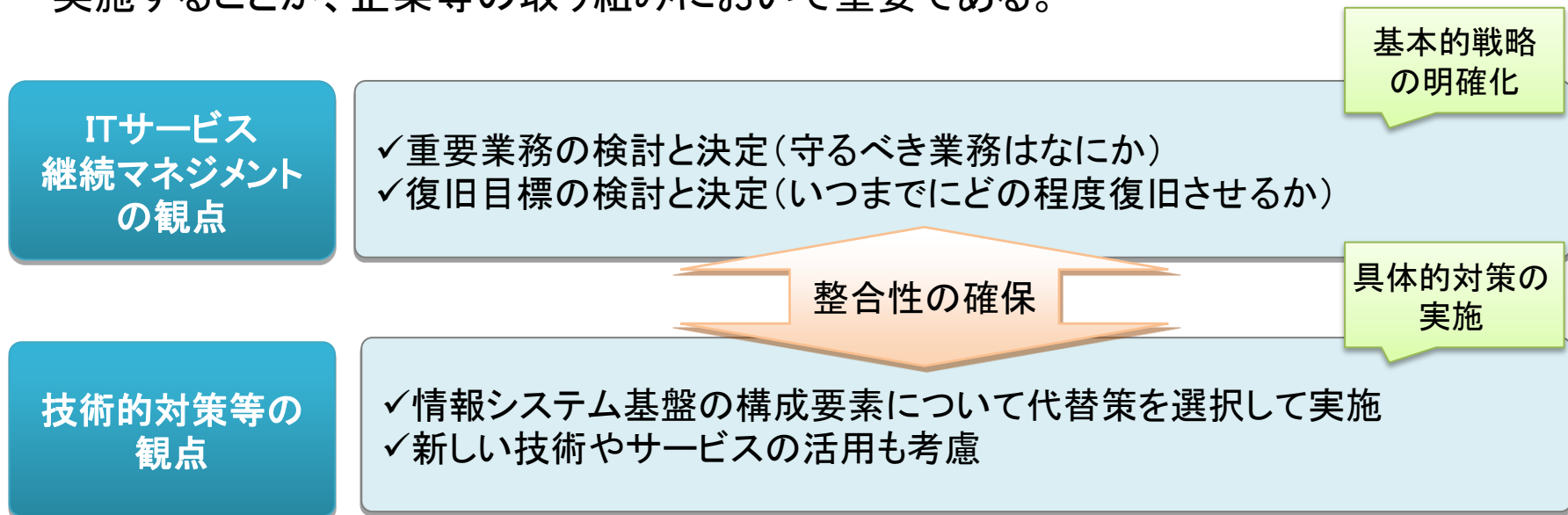
構成要素	対策		
業務アプリケーション・業務データ	・重要データについては遠隔地バックアップの実施。	・待機系システムの設置。	・バックアップサイトの設置。
OS・ミドルウェア	・遠隔地バックアップを含むバックアップの実施。		
ハードウェア機器やネットワーク機器	・代替機の用意(テスト機の活用等も含む)。		
建物、設備	・代替施設の準備。		
システム運用の体制や仕組み	<ul style="list-style-type: none"> <li>・システムに携わる要員の複数化(兼務要員の充当も含む)。</li> <li>・システム関連ドキュメントの整備と遠隔地保管。</li> <li>・復旧手順の整備。</li> </ul>		
通信	<ul style="list-style-type: none"> <li>・回線の冗長化、多様化。</li> <li>・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。</li> </ul>		
電力	<ul style="list-style-type: none"> <li>・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。</li> <li>・異なる電力管内におけるバックアップサイトの整備。</li> </ul>		

- システム構築に関して、仮想化技術やクラウド等の新しいサービスの活用も有効。

技術・サービス	活用の考え方
サーバ仮想化技術	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>
クラウドサービス	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>

## 5.4 ITサービス継続に関する基本的な戦略と 具体的対策の整合性確保

- システム基盤の復旧能力の向上のためには、各企業等の事業のIT依存度や経営資源の制約等を勘案した上で、最悪の事態を避けるための最大限可能な対策を実施する必要がある。
- 今回調査した事例の多くは、基本的戦略と整合のとれた復旧対策が実施されていた。
- アンケート調査結果からは、必ずしも両者の整合がとれていない例も散見された。
- 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、企業等の取り組みにおいて重要である。



→同様な考え方で復旧対策について解説している『高回復力システム基盤導入ガイド』の活用が有効と考えられる。