【研究グループ発表 】

保険会社におけるディザスタリカバリについて

～　Disaster Recovery for Insurance Company　～

ＩＴ研究会　第１グループ

＜担当委員＞

安達　秀樹　（ニッセイ情報テクノロジー）

田中　清長　（住友生命）

＜メンバー＞

岩淵　和紀　（オリックス生命）

加部　恵美子　　桝谷　宏　（ニッセイ同和損害）

森　徳光　　西川　覚　（ニッセイ情報テクノロジー）

庄治　貴弘　（大同生命）

吉田　晋久　　井上　和也　（住友生命）

＜目次＞

はじめに

近年各地での地震災害やテロ事件などを機に、災害対策の重要性が認識されるようになってきた。わが国の国土は、地質上においても気象上においても、さまざまな自然災害をもたらす条件下にあると言われており、過去数多くの地震や台風等の災害に見舞われている。昨今発生した事例を振り返ってみると、平成７年１月には、死者・行方不明者が６，０００人を超えた阪神・淡路大震災、記憶に新しいところでは平成１６年１０月の新潟県中越地震(被害総額約３兆円)、平成１７年４月には福岡県西方沖地震等が発生している。

企業のグローバル化が進んだ現今、ビジネス活動中断の影響は自社だけに留まらず、協業各社・取引先を巻き込むことを意味するため、災害時にも業務を継続できることが求められている。なかでも金融機関においては、一般の事業会社より公的な性格が強いため、災害によるサービス力の低下は経済的にも社会的にも問題となることは想像に難くない。

さらに、目下の銀行窓販解禁による販売チャネルの拡大に伴い、銀行等と同等の高い災害対策レベルが保険会社にも求められるようになってきた。

我々第１グループでは、保険会社各社の現状把握と、法的・社会的要求の整理、そして最新の技術動向の調査を行い、保険会社が目指すべきディザスタリカバリについて提言を行う。

第Ｉ章　ディザスタリカバリとは

この章では一般的な視点から、ディザスタリカバリの概要について説明を行う。

１．ディザスタリカバリの意味

ディザスタリカバリとは、直訳すると「災害復旧」となるが、一般的には「予期しない災害や天災によって受けたシステム障害から復旧・修復すること」という意味で使われ、直接的な災害対策全般を扱うのではなく、情報システムやＩＴ分野に絞った用語として用いられる。

これは、大震災やテロなどが発生した場合、情報システムは物理的にもデータ的にも大規模かつ広範囲にわたって被害を受けるため、一般的な障害対策だけでは復旧に時間がかかりすぎてしまう恐れがあるためである。情報システムの被災による企業への影響は、物的・人的資産の損失だけでなく「業務の停止」「重要データの消失」「社会的信用の失墜」など間接的・長期的な影響が非常に大きいために、「情報システムを復旧させること」は企業にとって特に重要な意味を持っているといえる。

よって、一般的な「災害復旧」や「防災」などとは一線を隔し、早急かつ確実にシステムを復旧できる体制を整備することを目的とし、ディザスタリカバリの体制を整えることが求められている。

２．災害時の被害例

実際に、情報システムが被災した場合の企業への影響について、阪神大震災を例に紹介する。Ｓゴム工業の関連会社は、同震災にて１ヶ月のシステム停止に追い込まれた。システムが使用できない期間は、従業員が紙で受注を受け、実際に目で見て在庫確認を行い、泊まり込みで注文に対応したという。しかしこうした旧来型のやり方では、従業員の粉骨砕身の働きにも関わらず、全く業務が追いつかず売り上げも立たなかったとのことである。

この会社は、１ヵ月後にバックアップテープからシステムを復旧させることができたが、万一システムを復旧することがあと数ヶ月できなかったら、企業の存続すら危ぶまれる事態になっていたと考えられる。システム化による人員の削減やシステム依存体質は、予想以上に大きいものだといえそうだ。

さらに、平成１３年９月に起きた米国同時多発テロにおける事例を紹介する。Ｌ金融機関は、旅客機が衝突した世界貿易センタービルの正面にあったデータセンターが機能しなくなった。災害対策については先進的に取り組んでいるアメリカらしく、川の対岸にバックアップサイトとなるデータセンターを構築していたため、バックアップの稼動は可能であった。しかし、バックアップデータをテープ媒体に強く依存していたため、復旧に時間がかかったことが課題として挙げられている。これは、災害時のシステムダウンだけが問題ではなく、災害復旧のプランについてもいくつか課題があることを示している。

３．災害対策への取り組み

（１）事業継続計画とは

前節のような災害に対する被害を未然に防ごうと、国内外で「事業継続計画を策定する」ということが盛んに叫ばれている。日本においては、内閣府の中央防災会議のガイドラインにおいて「事業継続計画策定」に努めることと明記されている。

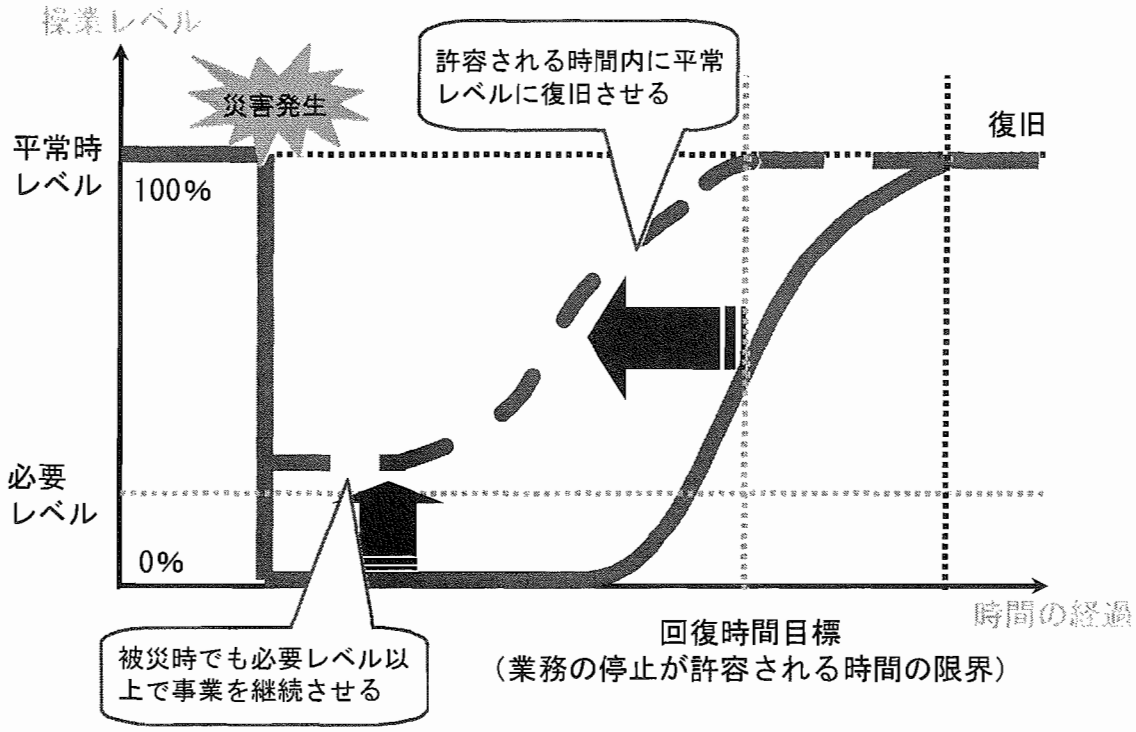
この事業継続計画はBusiness Continuity Planを略して「ＢＣＰ」と呼ばれるが、この意味は、企業・組織が事故や災害などの要因で被害を受けた際、

「主要なビジネス機能を継続できること」「できるだけ早く通常の業務を再開できること」

を目的として事前に取り決めた事項や手順ということである。具体的には、被災時でも重要業務を継続させる方法や業務の復旧の方法などをあらかじめ決定しておき、それが実行できるよう、組織体制や実施手順を確立しておくということになる。

（２）事業継続計画策定の目的

【図表Ｉ－３－(２)】事業継続計画の目的



このグラフ【図表Ｉ－３－(２)】は、縦軸に操業レベル、横軸に時間の経過をとり、被災時から業務が復旧するまでの変化を図示したものである。事業継続計画が策定されていない場合は、実線のモデルとなり、災害と同時に操業レベルが０％、つまり全く業務が出来ない状態まで下落することとなる。

ここで注目すべき点の一つ目が「必要レベル」である。多くの企業には被災などの非常事態であっても、最低限継続しなければならない業務があり、たとえば保険業界であれば「契約内容の照会業務」や「保険金の支払い業務」などが挙げられる。その主要な業務を継続できることが「必要レベル」を維持するということになる。

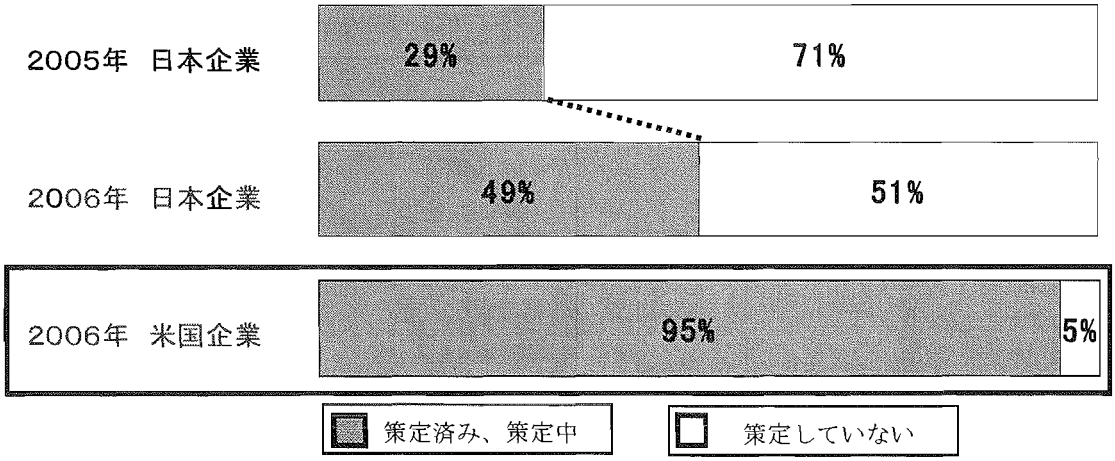
事業継続計画を策定していない実線の場合では、この必要レベルを維持することが出来ていない。そしてしばらく業務が出来ない状態が続き、その後徐々に回復していくという経過を辿るが、ここでさらに注目すべき二つ目の点が「回復時間目標」である。これは言い換えれば業務の停止が許容される時間の限界ということである。

たとえばある原材料メーカーでは、製造メーカーとのサプライチェーンの関係上、少なくとも被災後一週間で、通常通り業務が行えるようになる必要があるという場合、この「一週間」が回復時間目標ということになる。上記の例では、回復時間目標をオーバーしてしまっている。

事業継続計画を策定する目的は、この実線を点線のレベルに引き上げることである。事業継続計画策定後は被災直後でも必要レベルの業務を継続でき、かつ、回復時間目標以内に業務を平常時のレベルに回復させることが目標となる。

（３）事業継続計画への取り組み状況

【図表Ｉ－３－(３)－１】事業継続計画への取り組み状況



出典：KPMG Japan, BCMニュースレター （BCIジャパンアライアンス作成）
インターリスク総研 事業継続経営(BCM)に関する日本企業の実態調査報告書

上図の【図表Ｉ－３－(３) －１】は、日本企業の事業継続計画への取り組み状況である。国内では事業継続計画が策定済みまたは策定中の企業が、２００５年には２９％だったものが、２００６年の調査結果では４９％にまで増えている。これでも、米国企業の９５％には大きく遅れを取っているが、国内企業による事業継続計画の策定に関する認識は、高まってきているということが見て取れる。

また、近年事業継続計画について国内外の公的機関から以下の通り多くのガイドラインが発表されており、社会的・国際的にも事業継続計画の認知が広がっている。

【図表Ｉ－３－(３)－２】事業継続計画ガイドライン一覧

＜国内のガイドライン＞
○事業継続ガイドライン（内閣府中央防災会議）
○情報セキュリティに関する事業継続策定ガイドライン（経済産業省）
○中小企業 BCP 策定運用指針（中小企業庁）
○金融機関等コンピュータシステムの安全対策
（ＦＩＳＣ＜（財）金融情報システムセンター＞）
○金融機関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書
（ＦＩＳＣ＜（財）金融情報システムセンター＞）

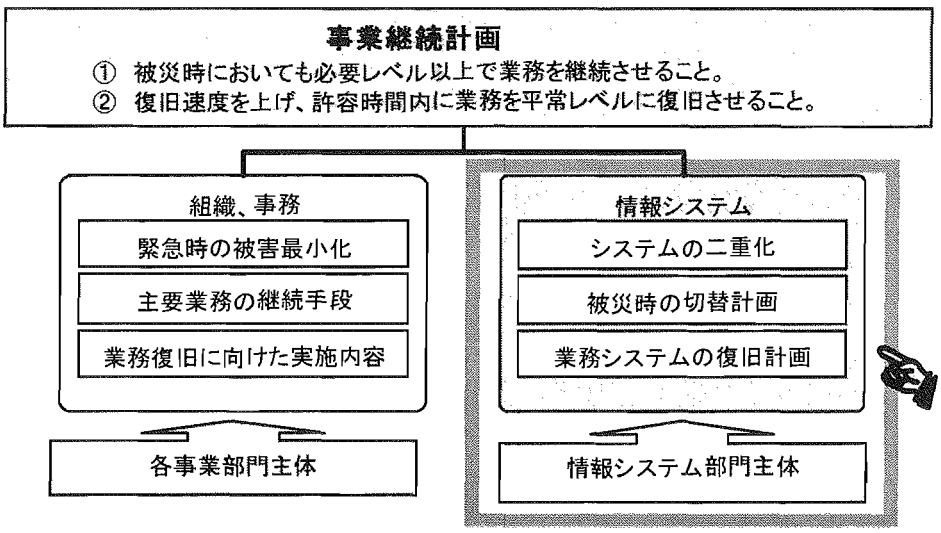
＜海外のガイドライン＞
○英国
ＢＳＩ／ＰＡＳ５６（英国規格協会）
○米国
ＡＮＳＩ／ＮＦＰＡ１６００　（米国規格協会）
○シンガポール
ＳＳ５０７　（シンガポール規格協会）

４．事業継続計画の策定

（１）情報システム見直しの必要性

実際に、事業継続計画の策定を行う場合、「組織」や「事務」の面の見直しが注目されがちであるが、「組織」や「事務」面の取り組みだけで、事業継続計画の目的を達成することができるのであろうか。先ほどの阪神淡路大震災の例からもわかる通り、現在の企業のシステムへの依存体勢を考えると、災害復旧計画は「組織や事務」と「システムの二重化」や「被災時の切り替え計画」「業務システムの復旧計画」といった情報システム面の災害復旧計画が十分であってこそ、初めて機能するものであると言える。よって、事業継続計画の策定には「情報システムの見直しが不可欠である」と考える。

【図表Ｉ－４－(１)】事業継続計画への取組体勢



（２）システム災害対策のポイント

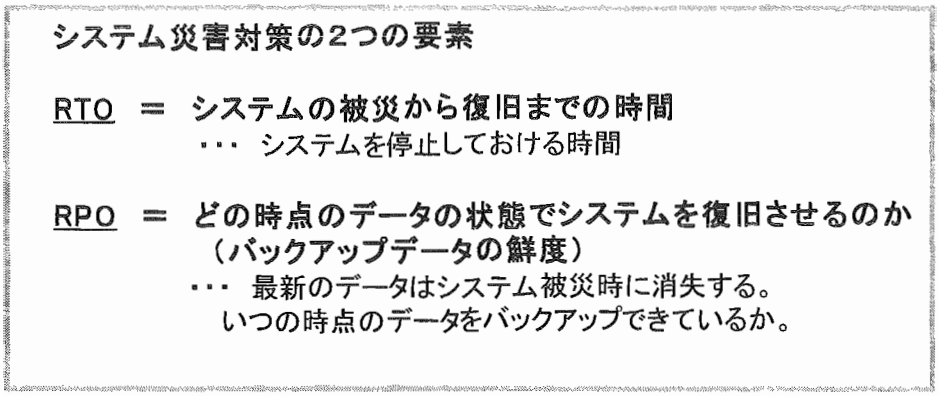
実際にシステムの災害復旧計画を立てる際には、大きく２点の要素を考慮し決定することが必要となる。一点目はＲＴＯといい、リカバリー時間目標と訳される。これは「システムの被災から復旧までの時間」である。「システムを停止しておける時間」と言い換えることもできる。たとえばある企業で「システムは被災から一日以内に復旧しなければならない」という要件があれば、ＲＴＯは２４時間ということになる。もしくは、株や為替のオンライン取引のように顧客ダイレクトで金銭を扱うような重要システムでは「システムは１０分以上停止してはならない」という要件があるかもしれない。その場合のＲＴＯは「１０分」ということになろう。

二点目はＲＰＯで、リカバリーポイント目標と訳される。システムの被災後、システムを復旧する際に「どの時点のデータの状態でシステムを復旧させるのか」ということである。システムの被災が起こった際復旧させるためにはデータが必要となるが、平常時に業務システムが稼動している間は、データは逐次更新されておりこれが最新のデータの状態ということになる。しかし、この最新のデータは被災を受けたと同時に消失するため、いずれかの時点でデータのコピーつまりバックアップを取得しておき、これを用いてシステムを復旧させる必要がある。

復旧されたデータは、その後業務の再実行や、更新ログがあればその内容を適用していくことで被災を受けた時点の状態に戻すことになるが、これは当然古ければ古いほど困難になってくる。「問題なく業務を再開するには、どの時点のデータでシステムを復旧させるべきか」ということをそのシステムのデータ更新の頻度や量、また処理の特性などから、決定しておく必要がある。これがリカバリーポイント目標である。

具体的には、１日前や３時間前など、またシステムによっては１分前などという要件もあるかもしれない。このリカバリーポイント目標は、つまりバックアップデータがどれほど新しいかということなので、「バックアップデータの鮮度」と言い換えることもできる。当然だが、はじめに説明したＲＴＯ：システムの復旧速度と、ＲＰＯ：バックアップデータの鮮度はどちらも短いほうが災害対策のレベルが高い、ということになる。

【図表Ⅰ－４－(２)】ＲＴＯとＲＰＯ



第Ⅱ章　保険業界の災害対策現状とあるべき姿

これまで述べてきたように、企業における災害対策の必要性は高まってきており、保険業界においてもそれは例外ではない。保険業界として災害対策のあるべき姿を考察するためには、まず災害対策の現状を整理することが重要であると考え、この章では保険業界とその他金融業界の現状を比較検証する事とした。

１．災害対策レベル

現状を把握するにあたり、まず指標となる災害対策のレベルについて、以下のように分類する。

【図表Ⅱ－１－１】災害対策レベル図

Level 1	データをテープで遠隔地に保管
Level 2	レベル１に加え、バックアップセンターを保持
Level 3	レベル２に加え、データを日次で伝送
Level 4	レベル３に加え、データを非同期伝送
Level 5	レベル４に加え、データは両サイトへの書き込みが完了してコミットされるDISKミラーリング方式
Level 6	２つのサイトが単一のシステムイメージで稼動、データはDISKミラーリング方式
Level 7	レベル６に加え、被災時はシステムの自動切換

各レベルの概要については以下の通りである。

Level 1 …　バックアップデータをテープに取得し、遠隔地に保管。このシステムが被災した場合、バックアップセンターが存在しないため、復旧のためにはシステムの構築作業から実施することとなり、最低でも数週間を要する。また２４～４８時間分のデータが消失。

Level 2 … Level 1に加え、バックアップセンターを保持。バックアップセンターの立ち上げには２４時間以上を要し、２４～４８時間分のデータが消失。

Level 3 … Level 2に加え、日次でデータ伝送を行うシステム。バックアップセンターの立ち上げは２４時間以内に行われるが、２４時間分のデータが消失。

Level 4 … Level 3のシステムに対してデータの伝送の頻度を上げたシステム。データの消失を３０分から６時間分に抑え、バックアップセンターは２４時間以内に立ち上げ可能。

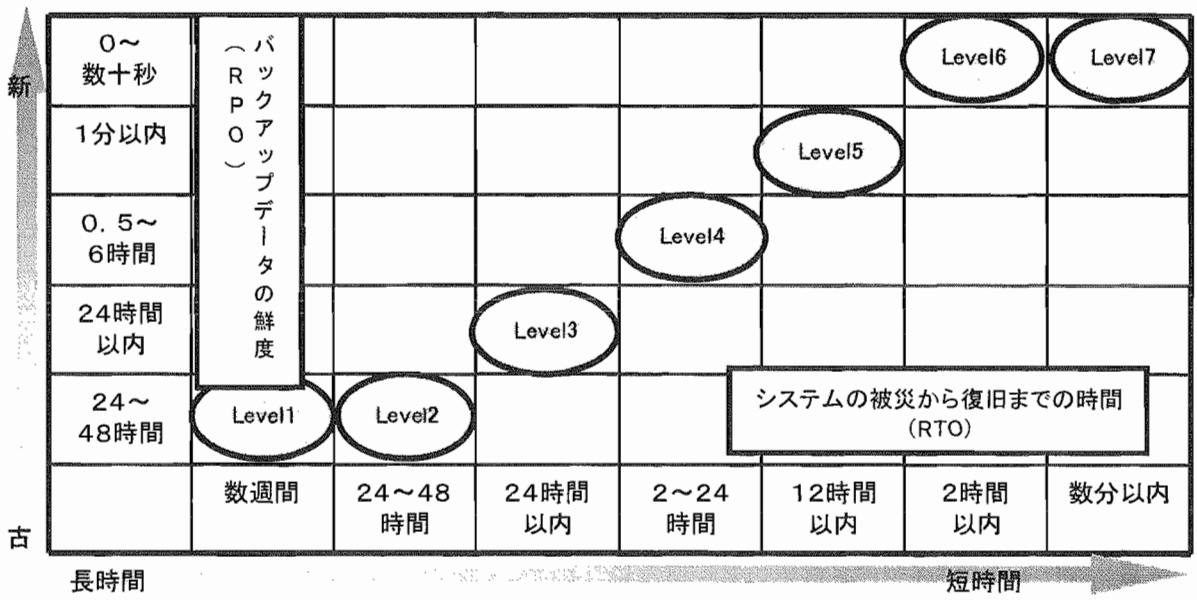
Level 5 … 業務の実行時に、離れた２つのセンター間のデータを同時に更新するシステム。被災時のデータの消失は、１分以下ときわめて小さく、バックアップセンターの立ち上げは１２時間以内。

Level 6 … ２つのセンターに「メイン」「バックアップ」という構成的な違いは存在せず、どちらも稼動系として使用可能なシステム。常にデータの同期を取っており、データの消失は皆無か、あったとしてもきわめて微少。立ち上げについては２時間以内で可能。

Level 7 … Level 6に加えて被災時にはオペレーションの必要が無く自動的に切り替えが行われるシステム。

なお、表に表すと【図表Ⅱ－１－２】の通りとなる。先に説明した、システムの被災から復旧までの時間とバックアップデータの鮮度を縦軸と横軸にとっている。右上に行けば行くほど、システムの復旧速度が速く、バックアップデータの鮮度が新しいシステムでありつまり「災害対策レベルが高い」ということである。反対に左下に行けば行くほど、「災害対策レベルが低い」ということになる。

【図表Ⅱ－１－２】災害対策レベル（７段階評価）



２．保険業界における災害対策の現状

保険業界の現状を把握するにあたり、当グループでは保険会社各社に対してアンケートを実施した。ここではアンケート結果の分析を行いながら、保険業界における災害対策の現状を解説していく。

（１）災害対策プランについて

まず現在の災害対策プランに関して質問を行った。（【図表Ⅱ－２－（１）】）

アンケート内容は「通常稼動しているメインセンターの機能が停止した場合の災害対策が計画されているかどうか」というものであったが、「策定されており周知されている」という回答が８４％にのぼり、各社とも災害プランは策定済みであるということが見てとれる。

次に、策定されたプランに基づいた定期的な訓練実施についての問いでは、「定期的に訓練を実施している」と回答があった割合は全体の７５％にのぼり、何らかの形で有事を想定した訓練は行われている結果となった。以上のことから災害対策計画ということに関して、保険会社各社とも何らかの対策を講じていることが判った。

（２）バックアップセンターについて

次に通常稼動しているセンターが被災し、機能が停止した場合に稼動させるバックアップセンター、もしくは同等の施設の有無について質問を行った。（【図表Ⅱ－２－（２）】）

その結果、施設が「ある」との回答が６５パーセント、「なし」との回答が３０パーセントに上った。上記によりバックアップセンターを保有している企業は約６割であり、構築されていない、つまり、データの保管のみ行っていると判断できる企業が３割に上るという結果となった。

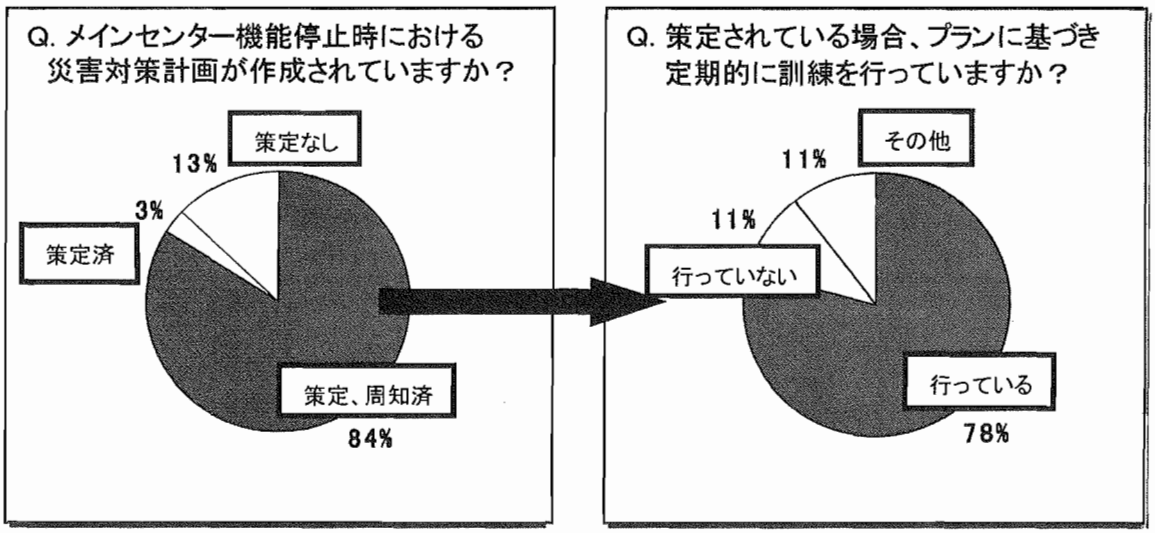
また、バックアップセンターが存在すると回答した企業に対して行った「バックアップセンターへの切り替えに要する時間について」の質問に対しては、２１社中１４社が１２時間以上と回答しており、立ち上げまでに１２時間（つまり１営業日以上）を必要とする企業が大多数であるという事が読み取れる。

最後に、データのバックアップ方式については、回答があった企業のうち「日次でのバックアップ」が７社となっており、保険業界では日次でのバックアップが主流という結果となった。

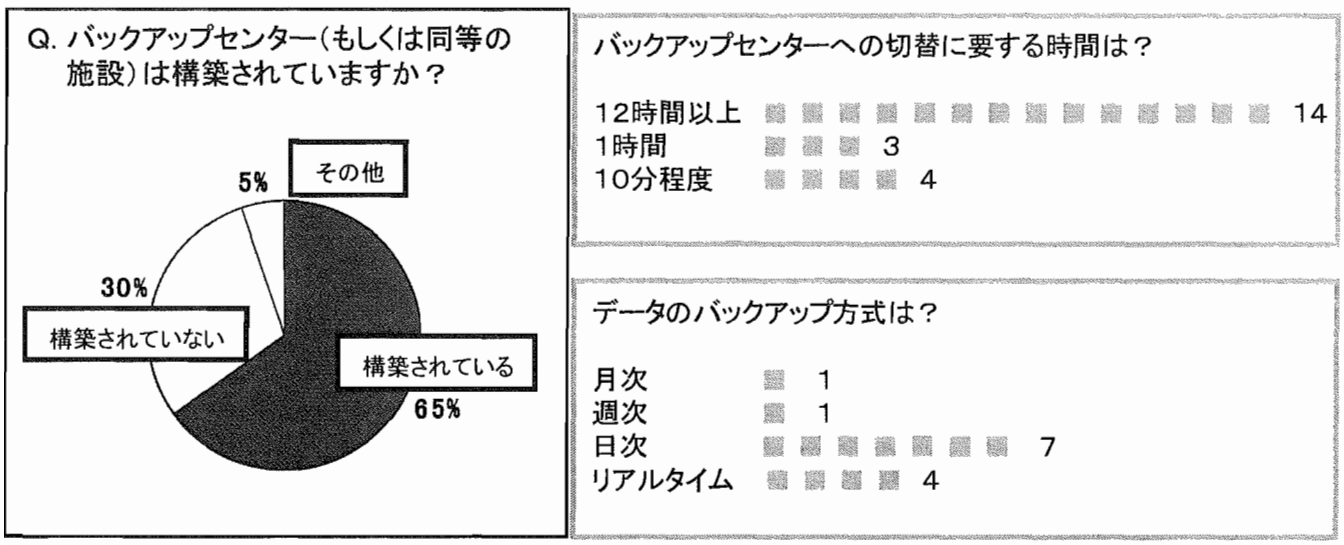
（３）保険業界の現状

これらのアンケート結果を受けて、保険業界の災害対策レベルが現在どのレベルに位置するのかという事を把握するため、【図表Ⅱ－２－(３)】の作成を行った。これにより、保険業界は一部高いレベルの災害対策システムを持つ企業が存在するものの、多くの企業がLevel 1およびLevel 3に属しているという結果になった。

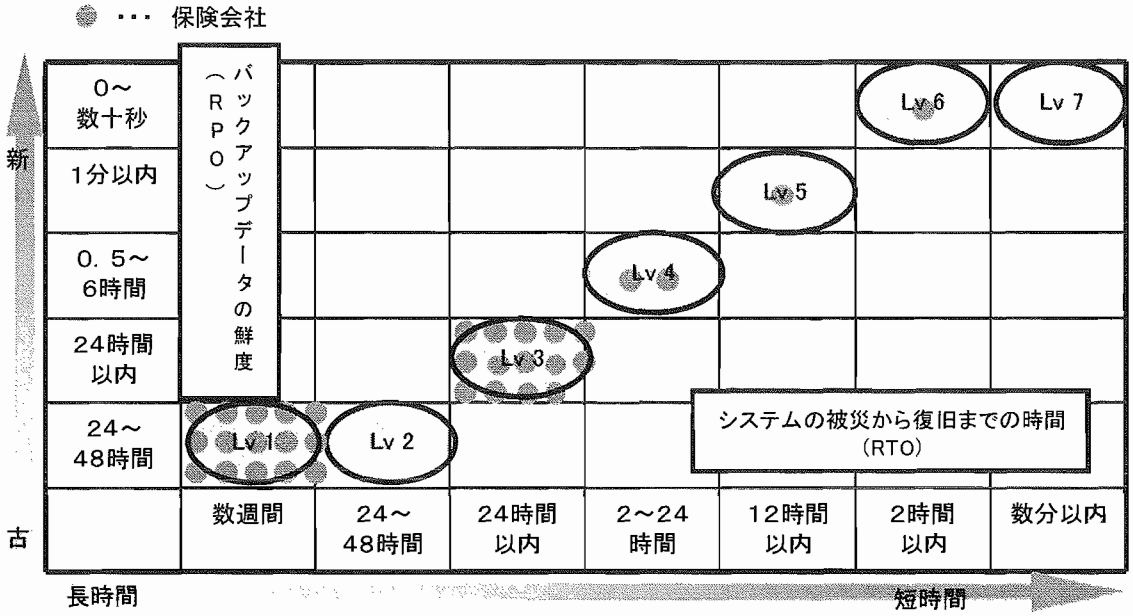
【図表Ⅱ－２－(１)】災害対策プランについて



【図表Ⅱ－２－(２)】バックアップセンターについて



【図表Ⅱ－２－(３)】保険業界の現状



３．金融業界の現状

前節では、現在の保険業界の災害対策レベルについて検証を行ったが、ここではその他金融業界での災害対策レベルについて解説する。金融業界を大きく「銀行」「信託」「証券」「損保」「生保」の５つに大別し、それぞれに属する代表的な企業について、現状を調査した結果は【図表Ⅱ－３】の通りとなった。
この資料の通り、「銀行業界」についてはLevel 6の災害対策を行っている結果となり、「信託業界」「証券業界」もこれを追随し、Level 6のシステムの構築段階であることが判明した。一方、一部上位の損保を除き、生損保の災害対策レベルはLevel 1～3となっており、保険業界は「銀行」「信託」「証券」業界に劣後していることは明白である。

【図表Ⅱ－３】金融業界の現状

		コンピュータセンターの配置	災害対策レベル
銀行	A銀行	関東圏－関東圏	◎ Level 6
	B銀行	関東圏－関西圏	◎ Level 6
	C銀行	関東圏－関東圏	◎ Level 6
	D銀行	関東圏－関東圏	◎ Level 6
信託	E信託銀行	関東圏－関東圏	◎ Level 6（対応中）
	F信託銀行	関東圏－関東圏	◎ Level 6（対応中）
証券	G証券	関東圏	◎ Level 6（対応中）
	H証券	関東圏－関東圏	◎ Level 6（対応中）
	I証券	関東圏－関西圏	◎ Level 6（対応中）
損保	J損保	関東圏－関東圏	◎ Level 6
	K損保	関東圏－関西圏	○ Level 4～5
	L損保	関東圏－関東圏	○ Level 4～5
生保	M生命	関東圏－関東圏	△ Level 3
	N生命	関西圏－関東圏	△ Level 3
	O生命	関東圏	△ Level 1

銀行・証券業界

・銀行業界
Level6 を達成済

・信託銀行、証券業界
Level6 対応を実施中

保険業界

・損保上位
Level6 を達成

・他社
Level1～3が平均的

４．保険業界をとりまく環境変化

元来保険業界のシステムにおいてはバッチ処理がメインであり、リアルタイムでデータを反映させる必要がある業務は、銀行などに比べて少数であった。被災時のシステム復旧までにかける事が可能な時間は、システムの処理形態、つまりリアルタイムでのデータ反映がどこまで求められるかということに依存する。このため保険業界においての災害対策は、他の金融業界に比べ優先度が低く扱われてきたと考えられる。しかし、近年の保険業界は集金事務のキャッシュレス化等により、以前よりはるかにデータ反映の即時化が求められるようになる等、環境が変化しつつある。また昨今の保険業界は、銀行窓販の全面解禁や郵政民営化等、外部環境の変化が激しい時期を迎えている。これに伴う販売チャネルの拡大が進みつつある現在、

・オンライン運用時間の拡大
・セキュリティ確保
・安定稼動
・災害対策

といった事が少なからずシステムへ影響を及ぼすと予想され、Ｊ－ＳＯＸ法やＢＣＰの国際標準化に向けた動きもあり、法的にも災害対策レベルの向上を今後求められるであろう。

５．あるべき姿

前節で述べたように、現在保険業界をとりまく環境は大きく変化している。「銀行」や「郵便局」が保険を販売する「代理店」となる事は、両者がお客様、つまりはシステムのユーザーとしての立場になると言える。

現在でも災害対策レベルが非常に高い銀行などからすれば、災害発生時にも平常どおりに業務が行えるよう、自社と同等の災害対策レベルを保険業界にも要求する事が考えられる。

以上から当グループでは、銀行レベルの災害対策を施すことが、保険会社のディザスタリカバリのあるべき姿であると主張する。

第Ⅲ章　「あるべき姿」を実現するシステム実装プラン

それでは、前章で述べた保険業界としての「あるべき姿」を実現するための技術的な側面として、具体的なシステム実装プランについて述べる。

１．現状の災害対策システム構成

各保険会社における災害対策の現状については、前述で述べたアンケート結果の通りであるが、ここでは各保険会社における現状の代表的な災害対策システム構成の特徴について具体的に解説する。従来の災害対策システム構成の特徴としては、【図表Ⅲ－１】の通りである。

まず、各保険会社で構築されている災害対策システムの構成としては、ほとんどがメイン／バックアップセンターの構成で構築されており、設置場所も東西二極分散や地域分散して設置している。しかしながら、多くの場合バックアップセンターはメインセンターのもつ全ての機能を保持しておらず、支払系業務を中心とした必要最低限の機能しか保持していないため、切り替え後も通常レベルの操業はできないシステムとなっている。また、被災時には手動で切り替える方式が主流となっており、システム切り替え時には手動切り替え作業が発生する。このため、切り替え作業には最低でも数時間～１日程度の時間がかかることになる。また、データの伝送方式としては、外部媒体（テープ）もしくはネットワークを利用した非同期データ伝送が主流であり、伝送サイクルは業務に応じて日次で伝送する方式である。このため、被災時は数時間～１日前のバックアップデータからの復元作業が必要であり、１日程度のデータロストが発生することになる。

【図表Ⅲ－１】従来の災害対策システム構成

【構成】
・メインセンター／バックアップセンター構成
【データ】
・外部媒体で日次伝送　　・ログデータの伝送
【アプリケーション】
・一部業務のみ搭載
【切り替え方式】
・作業員による手動切り替え
【特徴】
・被災時は数時間前のバックアップデータからの復元作業が必要
・切り替え時にはシステムの手動切り替え作業が発生
・バックアップサイトはメインセンターのもつ全ての機能を保持して
　おらず、切り替え後も通常のレベルでは操業できないシステムとなる

２．提案する災害対策システム構成案

これに対して、当グループで提案する「あるべき姿」を実現するためのシステム実装プランについて以下に解説する。システム構成の特徴としては、【図表Ⅲ－２】の通りである。

災害対策システムの構成としては、メイン／バックアップセンターの構成とするところは従来と変わりはないが、バックアップセンターの構成をメインセンター同等の構成とすることで、切り替え後も通常レベルの操業を可能とすることができる。メイン／バックアップセンターを同等の構成とする場合、同等の機器を導入する必要があるように思われるが、コスト削減方策として一例を挙げると、ＩＢＭ社の製品でCapacityBackupUpgrade（CBU）を活用する方法がある。この製品は、万一の故障や災害時にメインセンターの機器が使用できない場合に、バックアップセンター側の機器に搭載済みの処理能力を活性化するものである。この製品を活用すれば、メインセンター並みの機器を常時用意しておく必要がなく、大幅なランニングコスト削減が実現可能である。

また、データの伝送方式としては、ネットワークを利用した同期データ伝送を行う。これにより、メインセンターが被災した場合でもバックアップセンター側にデータ・ロスなく復旧することが可能である。切り替え時のデータ復元にかかる時間を短縮することで被災時の切り替え時間の短縮を図ることができ、現場の

業務への影響を最小限に抑えることが可能となる。同期データ伝送の技術としては、ＩＢＭ社のGDPS/GlobalMirror もしくは GDPS/Metro/GlobalMirror がある。GDPS は、並列シスプレックスを遠隔地間で実現する仕組みである。複数サーバをクラスタ接続して高可用性と高速処理を実現する並列シスプレックスを、遠隔地のサーバで実現する。これにより、メインセンターのシステム障害時に自動的に短時間でバックアップセンターに切り替えることが可能であり、自動的に CBU を活性化することも可能である。
GlobalMirror は、ＩＢＭのメインフレームである zSeries（z/OS、z/Linux）で利用できる高信頼性の高速非同期遠隔コピー技術である。距離制限はないが、その反面数秒程度のデータロスが発生する。MetroMirror は、zSeries（z/OS、z/Linux）に加えオープン系システムもサポートした同期遠隔コピー技術である。データロスはないが距離制限（最大３００Ｋｍまで）があり、距離に応じて本番システムへのパフォーマンスに影響がある。データ中継センターを新たに構築し、GlobalMirror と MetroMirror を組み合わせることで、距離制限なしでデータロスなしを実現することも可能である。
なお、本研究においては、ＩＢＭ社製の製品を中心に調査を行ったが、他社においても同等の製品があるものと考えられる。

【図表Ⅲ－２】新災害対策システム構成

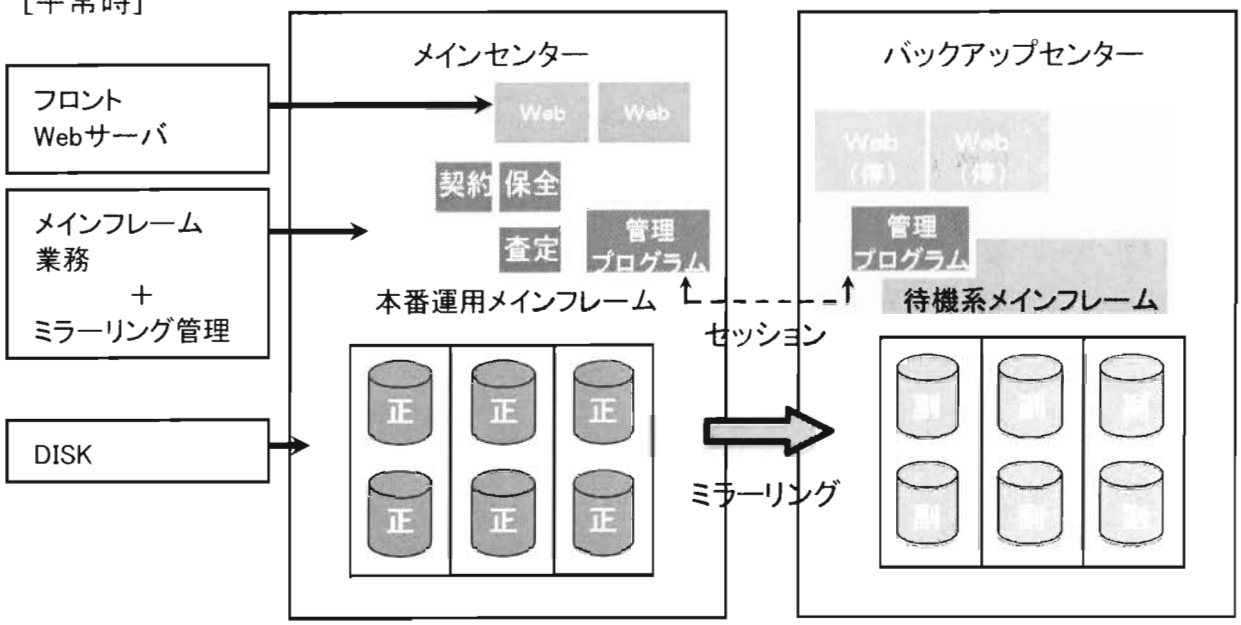
【構成】
・２センター構成
【データ】
・遠隔DISK間でミラーリング(同時更新)
【アプリケーション】
・全業務稼動
【特徴】
・最新技術である、遠隔DISK間でのミラーリングが可能な製品を採用
・切り替えはコマンド投入による自動切り替え
・平常時も両センターともに稼動可能
・二つのセンター間の距離制限有り
(ネットワーク環境により異なるが、システム制約上３００km程度が主流)

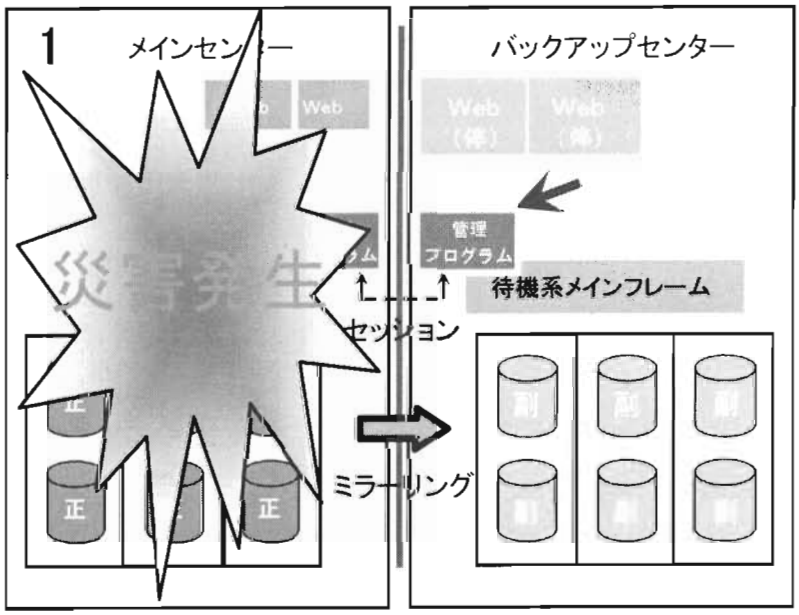
このようなシステム構成を採用すれば、データは常に同期され最新状態に保つことが可能となる。また、切り替え作業を手動ではなく「オペレータによるコマンド投入による自動切り替え」とすることで、オペレータの作業ミスのリスクを排除し短時間での切り替え作業が可能となる。

３．センター切り替えイメージ

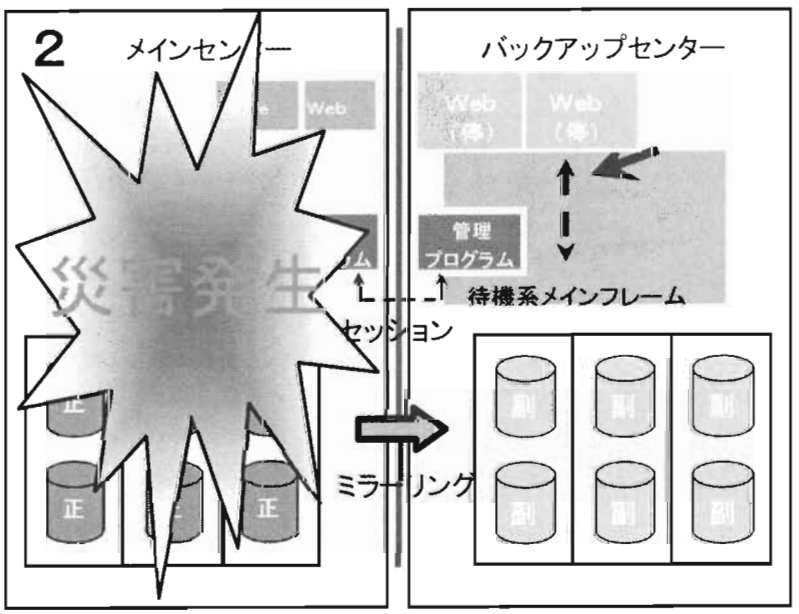
ここでは実際のセンターの切り替えイメージについて述べる。
例として挙げるシステムは、フロントとしてＷＥＢサーバが稼動し、メインフレームにて業務が稼動する構成とする。両センターの構成は同様であり、通常時は、メインセンターが稼動状態であり、バックアップセンターが待機系となる。バックアップセンターでは管理プログラムのみが稼動している状態となる。また、ＤＩＳＫはメインセンター／バックアップセンター間で前に述べた遠隔ＤＩＳＫミラーリングが行われている。
センター切り替えのポイントとして両センターで稼動している管理プログラムが挙げられる。この管理プログラムは、ＤＩＳＫミラーリング技術を基礎とした、総合的なシステム管理機能をもつプログラムであり、両センターの管理プログラムはセッションを持ち、常にお互いにセンターの情報をやり取りしている。これにより、いずれかのセンターに異常が発生した場合、もう一方もそれを検知出来るようになっている。
実際の被災時の流れは次の【図表Ⅲ－３】のようになる。災害が発生し、メインセンターが被災した場合、バックアップセンターで管理プログラムが異常を検知しオペレータに知らせる。オペレータは責任者に連絡を行い、連絡を受けた責任者はセンターの切り替え要否について判断する。切り替え要と判断した場合、オペレータにコマンド投入の指示を行う。コマンド投入実施後は、自動的に管理プログラムがバックアップセンターでメインフレームを活性化し、次にＤＩＳＫミラーリングを解消し、バックアップセンターの全ボリュームを副から正に変更する。オープンサーバのみを手動で立ち上げて、切り替えが完了となる。

【図表Ⅲ－３】センター切り替えイメージ



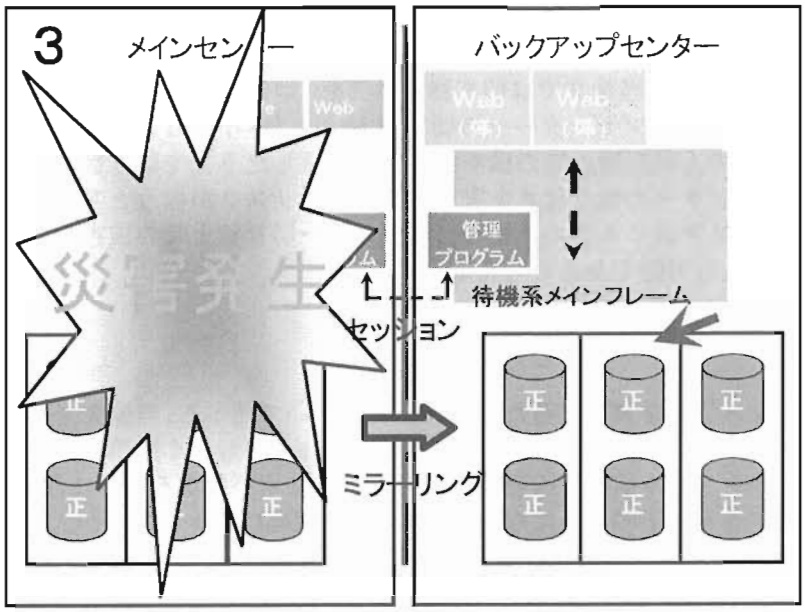


1. バックアップセンターで管理プログラムが異常を検知しオペレーターに知らせる。
オペレーターは管理プログラムにて被害状況を確認。
責任者による切替判断。
※　以下の手順はオペレーターのコマンド投入にて管理プログラムが自動実行



1. バックアップセンターで管理プログラムが異常を検知しオペレーターに知らせる。
オペレーターは管理プログラムにて被害状況を確認。
責任者による切替判断。
※　以下の手順はオペレーターのコマンド投入にて管理プログラムが自動実行

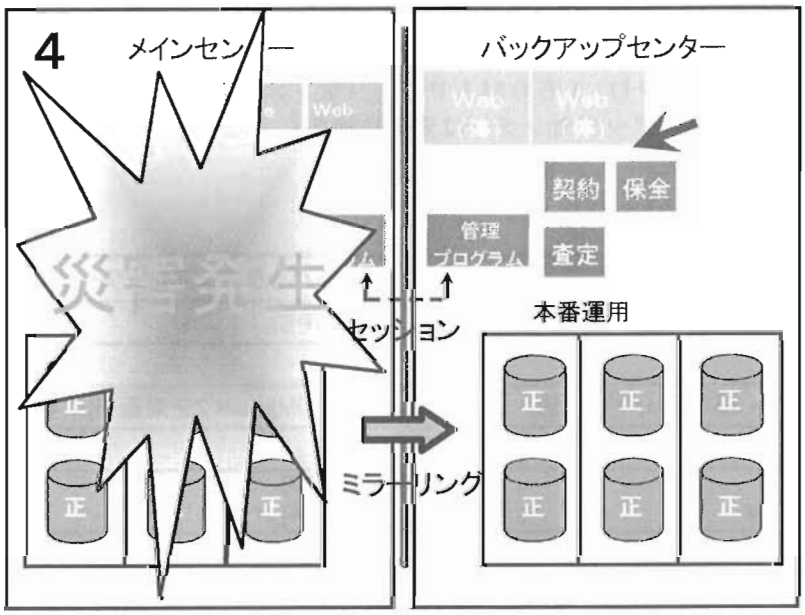
2. バックアップセンターでメインフレーム活性化



1. バックアップセンターで管理プログラムが異常を検知しオペレーターに知らせる。
オペレーターは管理プログラムにて被害状況を確認。
責任者による切替判断。
※ 以下の手順はオペレーターのコマンド投入にて管理プログラムが自動実行

2. バックアップセンターでメインフレーム活性化

3. Diskミラーリングを解消し、
全ボリュームを副から正に変更

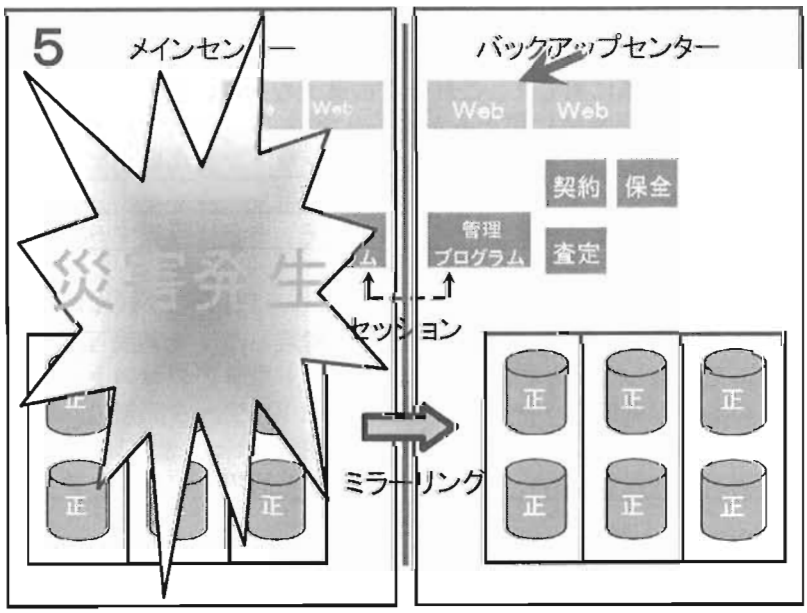


1. バックアップセンターで管理プログラムが異常を検知しオペレーターに知らせる。
オペレーターは管理プログラムにて被害状況を確認。
責任者による切替判断。
※ 以下の手順はオペレーターのコマンド投入にて管理プログラムが自動実行

2. バックアップセンターでメインフレーム活性化

3. Diskミラーリングを解消し、
全ボリュームを副から正に変更

4. 業務を起動



1. バックアップセンターで管理プログラムが異常を検知しオペレーターに知らせる。
オペレーターは管理プログラムにて被害状況を確認。
責任者による切替判断。
※ 以下の手順はオペレーターのコマンド投入にて管理プログラムが自動実行

2. バックアップセンターでメインフレーム活性化

3. Diskミラーリングを解消し、
全ボリュームを副から正に変更

4. 業務を起動

5. WEBサーバを手動で立ち上げ
業務オープン

なお、技術的には災害発生を機械的に捉え、切り替えることも可能である。仕組みとしては、あらかじめ管理プログラムにセンター切り替え実施の被害レベル(規模)を設定しておき、災害の発生時には自動的にセンターの切り替えを実施する仕組みになる。しかし、当論文では切り替え方法を「コマンド入力による切り替え」としている。理由としては、現在、バックアップセンターへの切り替え時に「メインセンターの災害からの復旧目処」「バックアップセンター側での人員配置」等の様々な影響を考慮したうえで切り替え判断が行われているため、機械的な判断のみでのセンターの切り替えを実施することはリスクが伴うと考えたからである。今後、「センター切り替えによるシステムリスクの見極め」、「センター切り替え時の被害レベル(規模)の設定」を行うことにより自動切り替えも可能であると考える。

４．システム構築費

これまで説明してきた２センター構成のシステムを実現するための構築費について述べる。当論文で提案しているバックアップセンターの機能は、メインセンターと同等とするため、現在、最も多く採用されているメインセンター／バックアップセンターのシステム構成での経費と比べ多大な費用が掛かることになる。

実際に２センター構成の構築費用を試算すると以下のようになる。保険会社の規模は様々であるが、当論文では試算対象を「ＣＰＵ」、「ディスク容量」、「回線速度」「ソフトウェア使用料」とし、メインセンターの機能を「ＣＰＵ：５００ＭＩＰＳ」、「ディスク容量：５ＴＢ」、「回線速度：１Ｇbps×２」（メインセンターとバックアップセンターは 60km 程度の距離に構築）と仮定する。この場合の構築費用はメインセンターと同様の構成となるため、一時経費が約７億円、経常費用は約 2.1 億円／年となる。

一方で、従来のバックアップセンターではメインセンターと同等の機能を有していないため、メインセンター機能の３分の１とする。この場合の費用は、「ＣＰＵ：１５０ＭＩＰＳ」、「ディスク容量：１ＴＢ」、「回線速度：１０Mbps×２」（メインセンターとバックアップセンターは東阪に構築）となり、一時経費が約 1.9 億円、経常経費が約 0.9 億円／年となる。

【図表Ⅲ－４－(１)】概算構築コスト

	【我々の提言(メインセンターと同規模)】	【従来のバックアップセンター】
CPU	5.0億円（500MIPS）	1.5億円（150MIPS）
ディスク	2.0億円（5TB）	0.4億円（1TB）
回線	0.6億円／年（1Gbps×2を60km内に敷設）	0.4億円／年（10Mbps×2を東阪間に敷設）
ソフトウェア使用料	1.5億円／年	0.5億円／年
合計	一時経費 7.0億円 経常経費 2.1億円／年	一時経費 1.9億円 経常経費 0.9億円／年

５．投資に対する考え方

バックアップセンターを構築する際の必要投資額としては、前述のコストに加え、コンピュータセンター自体を新設する場合には約 50～100 億円程度の不動産経費がかかることとなる。

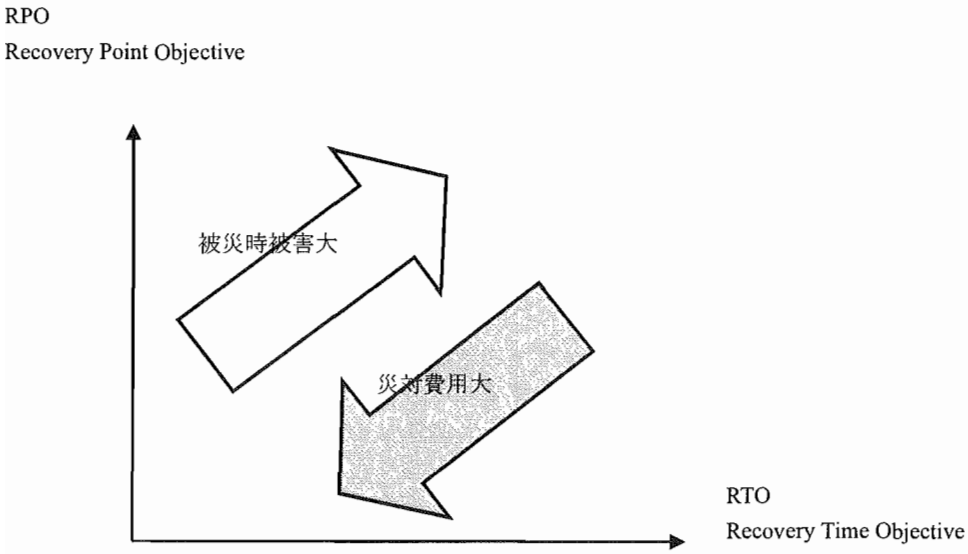
「災害」といういつ発生するかわからない不確定事象に対して、これほどの莫大な投資を行うことは、従来の経営感覚（費用対効果による投資判断）からすると無駄に思えるかもしれない。

しかし、銀行窓販の全面解禁や郵政民営化による保険販売チャネルの拡大やオンライン運用時間の拡大要望などを踏まえると、保険業界においても銀行や証券などの他業界と同様の災害対策レベルが求められるのは時間の問題であり、景気回復を背景に各保険業界の業績が復調傾向にある今こそ、まさに投資すべき時期にきていると考える。

下図【図表Ⅲ－５－(１)】でもわかるように、災害対策に投資を行うことにより、「ＲＰＯ・ＲＴＯ」は短縮され災害による被害が小さくなるのは明らかであり、確実に銀行並みの災害対策レベルを実現可能である。また、これまでは、データ同期のシステムを構築しようとすると、回線やハードウェアのコストが大きく実現が困難であったが、近年、回線コストの急速な低減、ハードウェア価格の低下、データ同期のための製品の充実などが進んだことにより、以前に比べ比較的安価なコストで導入が可能になってきている。

このような状況を踏まえ、我々は今こそ災害対策に投資を行い、メインセンターと同規模のバックアップセンターを構築すべきであると提言したい。

【図表Ⅲ－５－(１)】コストと被害



おわりに

保険会社の情報システムは、大量の顧客データや保険料の複雑な計算ロジック、膨大なバッチ処理などを保有し、ハードウェア・ソフトウェアの両面で大規模かつ複雑なものになっている。これは災害対策を施すという観点では、銀行など金融他業種と比較しても非常に困難なシステムであるといえる。また、これまで保険業界では、災害対策はある意味軽んじられ、業界で包括的な議論が行われることもなく、各企業がコスト前提や金融庁対策など独自の観点で様々に異なったレベルの災害対策システムを構築してきた。

しかし、災害対策の本懐は「災害時にも企業活動を継続させ、社会的責任を果たす。」ということに他ならない。とりわけ、保険業界は公的性格の強い業務特性からも、その責務は非常に重く、また企業規模の大小にかかわらず同一のはずである。よって、業界全体が高度な災害対策レベルを達成する必要があることはこれまでも述べてきた通りである。

「他企業には類を見ない大規模・複雑な情報システムを保有しつつ、一方で重大な社会的責任を負うという、ディザスタリカバリの観点において相反する要素を持ち、また、現在外部環境の変化に伴って大きな変革を迫られている。」このような状況は、保険会社各社に例外なく共通するものであるという認識を、我々は研究を通して強めた。

そして、災害対策はこれまでのように一社で取り組むべきものではなく、業界全体の共通課題として改めて捉え直す必要性を大きく実感している。

今後、災害対策について企業横断的な協力体制の下、さらなる研究、議論が行われること、そして、我々第１グループの取り組みがその先駆けとなろうことを切に願って、結びの言葉とさせていただく。

＜＜参考文献＞＞

・「日経 BP」
http://www.nikkeibp.co.jp/sj/it/02/03.html

・「事業継続経営（ＢＣＭ）に関する日本企業の実態調査報告書」
著／インターリスク総研　KPMG Japan,　BCMニュースレター
（BCIジャパンアライアンス作成）

・「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書（第３版）」
著／FISC 金融情報システムセンター

・「特定非営利活動法人　事業継続推進機構」
http://www.bcao.org/index.html

・「FISC 金融情報システムセンター」
http://www.fisc.or.jp/about/

・「金融庁」
http://www.fsa.go.jp/

・「フリー百科事典『ウィキペディア（Wikipedia)』」
http://ja.wikipedia.org/wiki

・「Japan.internet.com」
http://japan.internet.com/public/technology/