特定非営利活動法人　日本システム監査人協会　近畿支部

BCP研究会活動報告

ＩＴを中心とするＢＣＰ策定支援の実践

SAAJ 西日本支部合同研究会

2011年11月19日

BCP研究会　荒町　弘

研究会メンバー

[主査]
荒町　弘　　(株式会社 内田洋行)
[副主査]
川端　純一　　(株式会社 ＪＫソリューションズ)
[主要メンバー]
岩佐　修二　　(経営とITコンサルタント　Office　イワサ)
尾浦　俊行　　(奈良県)
大塚　一志　　(株式会社 シーエーシー)
金子　力造　　(企業経営に関するITコンサルタント)
木村　安寿　　(関西学院大学大学院)
是松　徹　　(オムロン株式会社)
関西　康一郎　　(創玄塾)
野末　泰弘　　(マネジメントオフィス野末)
吉田　博一　　(大阪府)

(敬称略　５０音順)

目次

＜第1部　研究会発足～A社共同に至る経緯＞

研究会発足の経緯

- 2010年度　近畿支部総会後の情報交換会にて近畿支部関西理事より提案があった
- 発起人3人がメンバを募り2010年2月17日にキックオフ→研究会発足へ
- 当初メンバは8名でスタート
- まずは参加メンバの知識共有から開始
- BCP策定支援アドバイザーの仕事を手掛けておられる川端理事にレクチャーをお願いする

目標設定

- WGを進めるにあたり、目標を設定。

1．研究会メンバとしてＢＣＰに関する知識と理解を深める。

2．ITのビジネスリスクやリスク分析について意見交換し見解をまとめる。

3．中小企業にフォーカスしたリスク対応ケースを作る。

具体的な研究内容の検討

- リスク分析をどのようにすればよいか？
  (いきなりBIA (ﾋﾞｼﾞﾈｽ影響度分析) はハードルが高すぎるのでは？)
- 何をベースにしたBCPがよいのか？
  (BCAOのステップアップガイド・・・全社的BCP？)
- 対象企業の規模や、業種は？
  (大企業のBCPは専門部署が組織化されている)
  (システム監査人として研究するならICT分野に特化したほうが・・・)
- 参考資料等は何を用いるべきか・・・
  (BCAOのBCPｽﾃｯﾌﾟｱｯﾌﾟｶﾞｲﾄﾞのｱｳﾄﾌﾟｯﾄを埋めることが目的？・・・)
- BCP策定活動内容がいまひとつ具体化できない・・・
  (実際の企業におけるBCP策定支援活動を通じて研究を進められれば・・・)

リスクに対する認識の整理

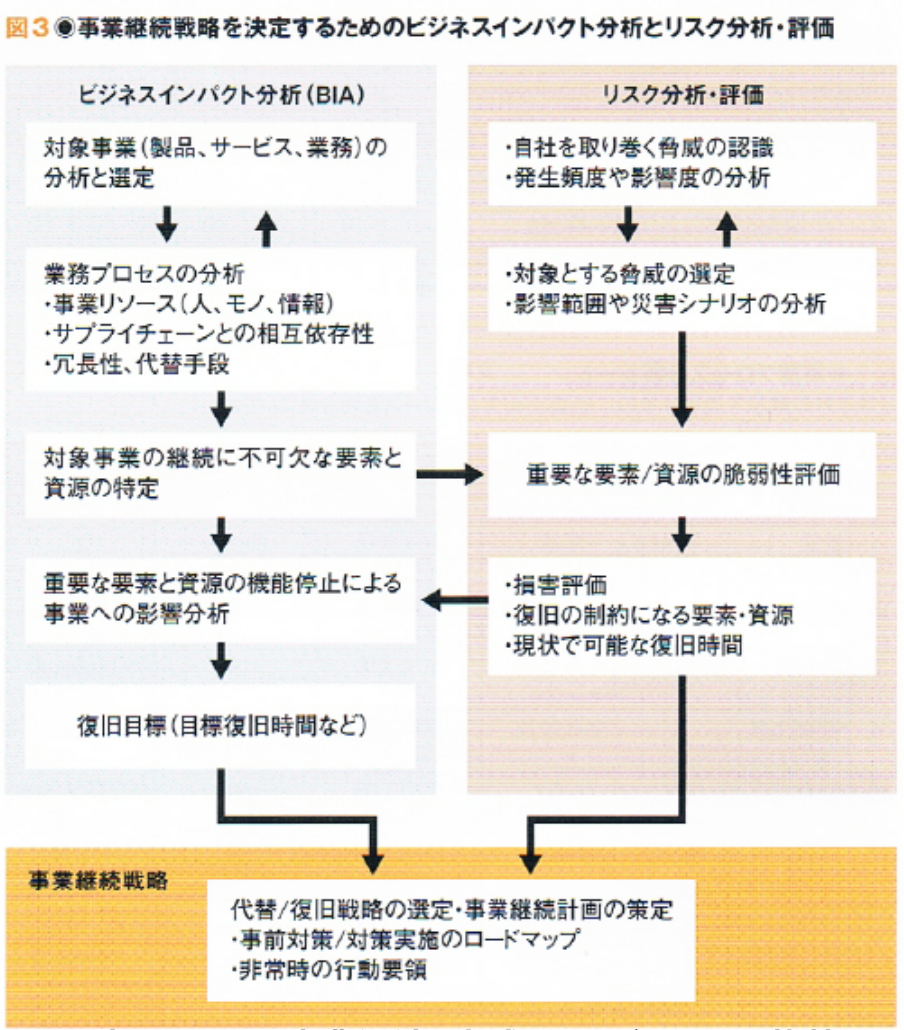
BCP策定への取組みとしては、下記の作業を並行して行うことが必要。

1. **ビジネスインパクト分析**
2. **リスク分析･評価**

しかし、具体的な分析を我々が行うことは不可能である。

中小企業にとって、BCP策定に多大な時間と経費をかけることは困難である。

良い方法はないものか？？？



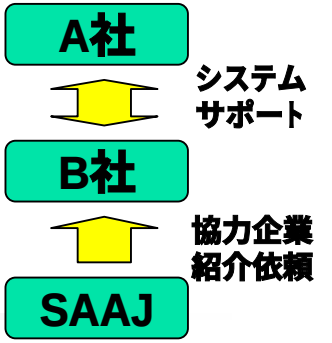
「日経-ビジネスを止めるな！　事業継続　実践ガイドブック」より抜粋

協力企業（A社）との接点・アプローチ

- 2010年6月（第3回WG）より協力企業を交えての取組みについて協議を始めた。
- より、実効性のあるBCP策定への取組みは、実際の企業との協同作業が最も近道であるという認識に至る。

- 協力企業をいかに探すか？
- 協力企業とSAAJの双方がWinWinの立場で取り組めるためには？

協力企業（A社）との接点・アプローチ



① BCPへの取組みに協力頂けそうな企業（A社）を紹介して頂く。（取引先B社に依頼）

② A社へのアプローチに際して、取引先B社へ趣旨説明を実施（8月初旬）。

③ A社への初回訪問と趣旨説明（8月中旬）。

④ A社内にて経営層を含めた検討を頂く。

⑤ BCP策定の協同取組みに対してA社より承諾を得る（9月）。

協力企業（A社）への提案内容

1．取組みの目的

貴社の顧客に対するサービス等の事業活動の継続性を維持し、損失を防ぐためのＢＣＰ策定支援を行います。具体的には貴社の上記重要業務を担うITシステムおよびIT部門の事業継続計画策定を実施します。

事業継続・企業の利益を守る

2．取組みの内容（ＢＣＰ策定に向けた活動）

中小企業ＢＣＰステップアップ・ガイド（4．0版）の第1部「ＢＣＰの基礎になる防災対策の実施」をもとに計画策定を行います。対象範囲は貴社IT部門と重要業務を担うITシステムとします。

IT部門と重要業務システムを対象

3．スケジュール

活動期間　：　2010年9月から2011年3月までを活動期間とする。
（詳細は協議のうえ、決定させて致します）

無理のないスケジュール

4．成果品

中小企業ＢＣＰステップアップ・ガイド（4．0版）にて提供されている様式を基本に用いた成果品を作成いたします。

既にあるガイドラインを用いた取組み

5．その他（経費等）

基本的に貴社の費用負担は発生いたしません。
貴社への往訪以外に経費が発生する場合は別途実費のご負担をお願いする場合がございます。

費用は頂かない

＜第2部　A社概要とBCP策定支援活動について＞

A社の概要（企業とITの概要）

- 「化学系」に関する取組みを行う企業
- 全国に約20箇所の事業所を持つ
- 全国に機械工場・化学工場・物流拠点を持つ
- 全社のITは本社ICT部門が担当（メンバ3名）
- 約30台のサーバは近畿圏の事業所にて一括管理
- 全社ネットワークは某通信事業者の光サービスを用い、バックアップ回線としてＡＤＳＬ網も整備
- 基幹業務システムはメタフレーム(*)により運用
- 基本的にクライアントに資源を置かない構成
- 社内のサーバや端末はインターネット接続できない

(*)メタフレーム ・・・ Citrix Systems社が開発した、Windowsサーバが備えるターミナルサービスを利用するためのクライアントプログラム。（IT用語辞典より）

A社の概要（BCP策定に向け）

- 少ないマンパワーでの取り組みである
- 本社ICT部門の3名（うち実務2名）が月に割ける時間は延べ12時間（1.5人日程度）
- 実施にあたっては基幹業務のサポートベンダにも協力頂く（ドキュメント整備など）
- 活動の頻度は月1回とし、SAAJのWGに共同参加という方式にて進める

A社の概要（既存の課題など）

- 3名という少人数で全社のITを管理するため、**ドキュメント整備等が追いつかない**

  （セキュリティポリシーは策定したが、ドキュメントが最終纏め切れていない）
- 日常の管理については十分こなせているが、ドキュメント類を中心とする既存システムの**情報資産の整理が十分できていない**
- BCP策定を機に**既存システムの棚卸しも改めて実施したい**

A社との契約など（覚書と契約）

- A社とSAAJの間で下記書類の取り交わしを行った

1．ICT部門の業務継続計画（BCP）策定支援サービスに関する覚書

2．機密保持契約書
（A社書式）

A社のBCP策定支援活動

- 参考とするガイドラインの検討

  「地方公共団体におけるICT部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」を用いる

  ＜理由＞ICT部門に特化したガイドラインであるためA社の取組み範囲と一致する。アウトプットサンプルも提供されているため、取組みしやすい。

- 作業の範囲とアウトプット

  「上記ガイドラインにおける第1部（BCP策定の基盤づくり）を作業の対象とする」

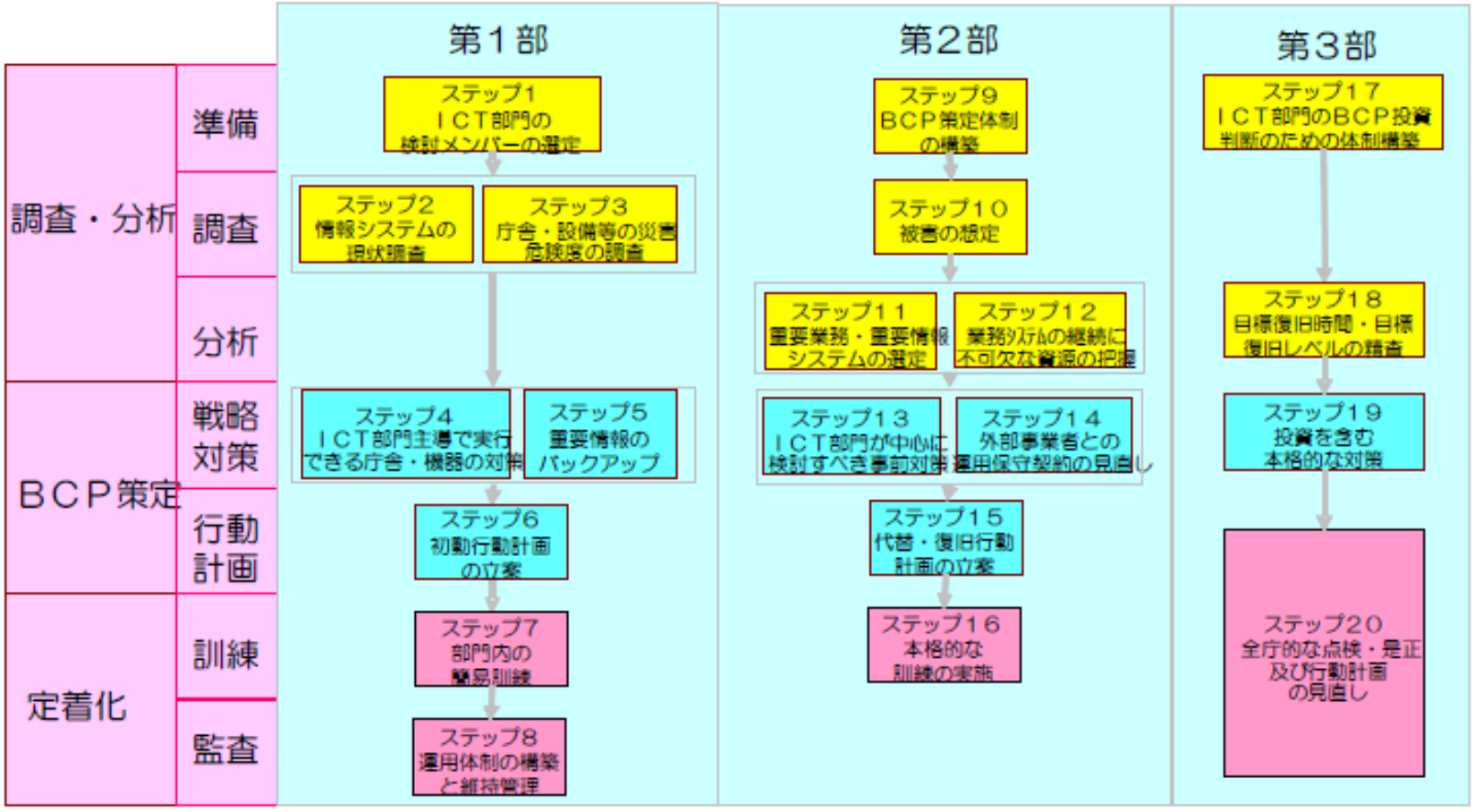
  「アウトプットについてもガイドラインのサンプルを参考にし、項目の追加などA社に必要な修正を加える」

- 作業主体とSAAJの役割

  BCP策定作業はA社が主体となり実施する

  SAAJは作業の過程において必要な助言などを行いBCPの精度向上に向けた支援を行う

ガイドラインのステップ構成



「地方公共団体におけるICT部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」より抜粋

「地方公共団体におけるICT部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」より抜粋

＜第3部　具体的な活動内容＞

WGの活動経緯とキーイベント

- 2010年2月　WG発足
- 2010年8月　A社へアプローチ
- 2010年9月　A社の承諾を得る
- 2010年10月A社との合同WG開始(第8回～)
- 2011年2月　A社電算室視察＆現地WG開催
- 2011年4月　ITC部門のBCP策定開始
- 2011年6月　ドキュメント中間確認（第14回WG）
- 2011年8月　ドキュメント整備（重要システムの事業継続方針）実施
- 2011年9月　ドキュメント整備（重要システムの事業継続方針）実施
- 2011年10月　ドキュメント整備（重要システムの事業継続方針）実施
- 2011年11月　ドキュメント整備（重要システムの事業継続方針）実施

BCP策定に向けた取組み

- 重要業務（システム）の選定
- 優先順位づけ
- 運用状況の確認
- **現地視察・サーバ室確認**
- 改善ポイントの洗出し
- ドキュメントの整理
- BCP（簡易版）の作成

	様式名
様式１	情報システム一覧
様式２	外部事業者との関係整理
様式３	庁舎（建物）の状況把握結果
様式４	システム機器設置場所の状況把握結果
様式５	電力供給、通信手段に関するリスクの把握結果
様式６	現状の脆弱性と対策の実施計画
様式７	重要情報のバックアップの状況と対策計画
様式８	緊急時対応体制
様式９	緊急連絡先一覧
様式１０	緊急時における行動計画（初動・代替・復旧行動計画）
様式１１	被害チェックシート　簡易版
様式１２	訓練計画
様式１３	業務継続計画の運用体制

「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」より抜粋

現地視察･サーバ室確認

管理･運用状況の点検

自家発電設備	敷地内駐車場屋根に太陽光発電設備を整備
電源設備	サーバ等全てUPS給電･停電時は太陽光発電にてサーバ室給電
地震対策	建物は新耐震基準に対応 サーバ室19インチラックは3台連結、転倒防止措置（スタビライザ） サーバ室内ラック以外の耐震･転倒防止措置（＊）
空調設備	サーバ室専用で空調有り エアコンからの漏水対策を検討（＊） 室外機の地上からの高さを上げるのが望ましい（＊）
配線設備	ケーブルラックによるラック上部配線 強電と弱電の配線区画化などは配慮が必要（＊）
水害対策	事業所が高台に位置し、河川氾濫による被害等は少ないと考えられる
火災対策	電算機用の消火設備を検討が必要（＊）

（＊）部分は今回の点検から検出された改善ポイント

現地視察･サーバ室確認

管理･運用状況の点検

環境監視	煙探知機有り、緊急時通報システムは自社開発（近々設置） 温度･湿度等の記録にはロガー設置（＊）
雷対策	建物自体の避雷設備のみ
入退室管理	サーバ室にはICT部門担当者と事業所責任者のみ許可
媒体管理	バックアップ媒体はサーバ室内に管理 区画された別の場所への保管を検討（＊）
建物の耐震	新耐震基準に対応
オフィス環境	５Ｓが徹底されている 無線ＬＡＮにより機動性の高いオフィス

（＊）部分は今回の点検から検出された改善ポイント

システムとデータを管理するサーバ室のファシリティ面においていくつかの改善ポイントはあるが、高いセキュリティ意識とIT部門の統制が効いており、運用状況の面では十分であるといえる。

東日本大震災の影響
(東日本の事業所にて)

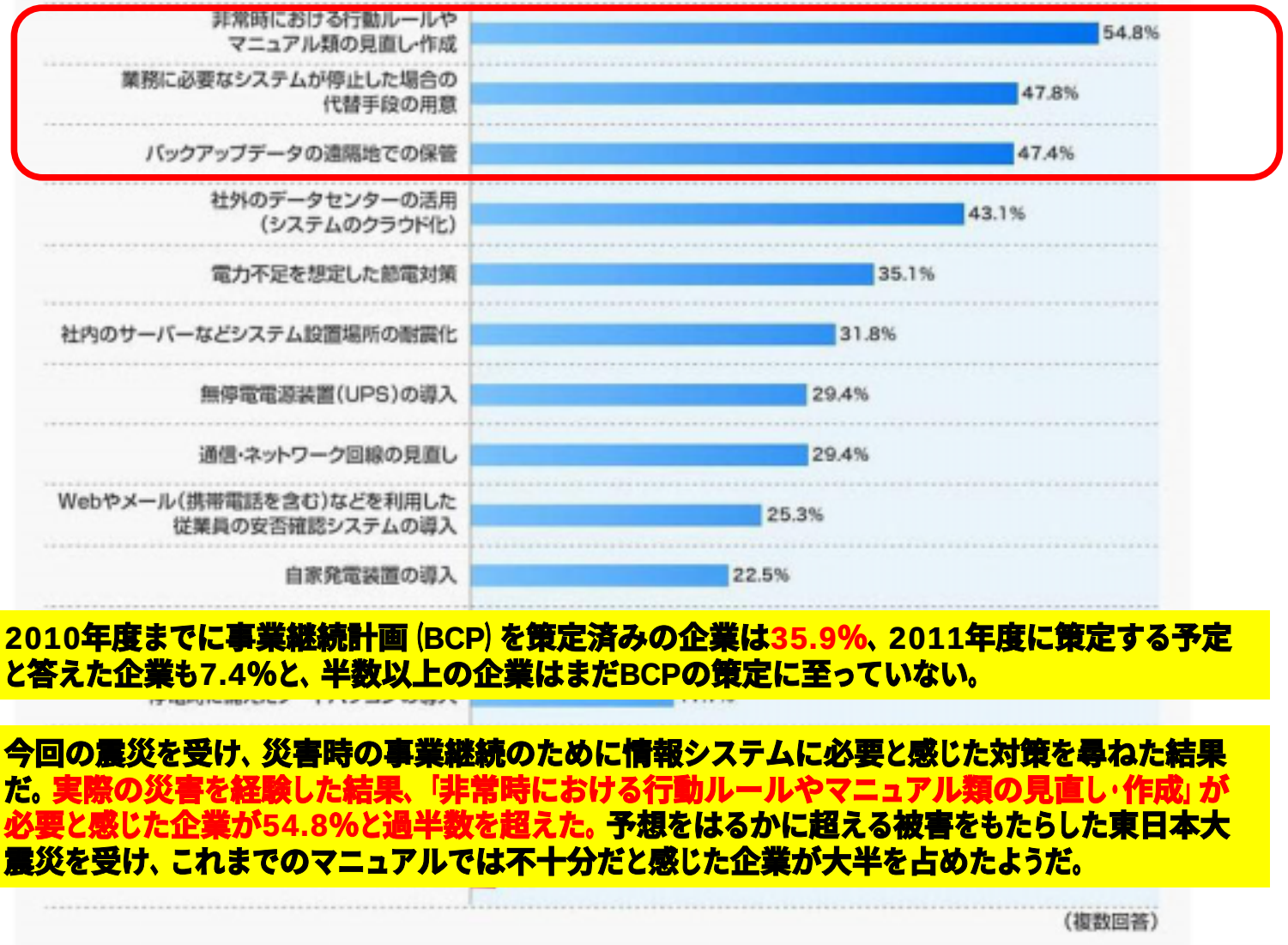
- 人的被害は無かった
- 関東の事業所が被害にあった (保険により解決)
  - 建物自体は無事だが、地盤沈下等の影響はあった
  - 隣接する建物の壁やガラスが飛来
- 化学品製造設備への影響
  - 製造ラインが停止、また、原材料の調達が不可能に
- 計画停電の対象となり操業が困難に
- 幸いにもITへの影響は無かった

西日本の製造設備の操業率を上げることにより、東日本の製造分を西日本からの供給でカバーし、サプライチェーンを維持することができた。

2011年6月30日の記事（記事提供：日経パソコン）より

日本経済新聞 - Windows Internet Explorer

災害時の事業継続に必要と感じた対策

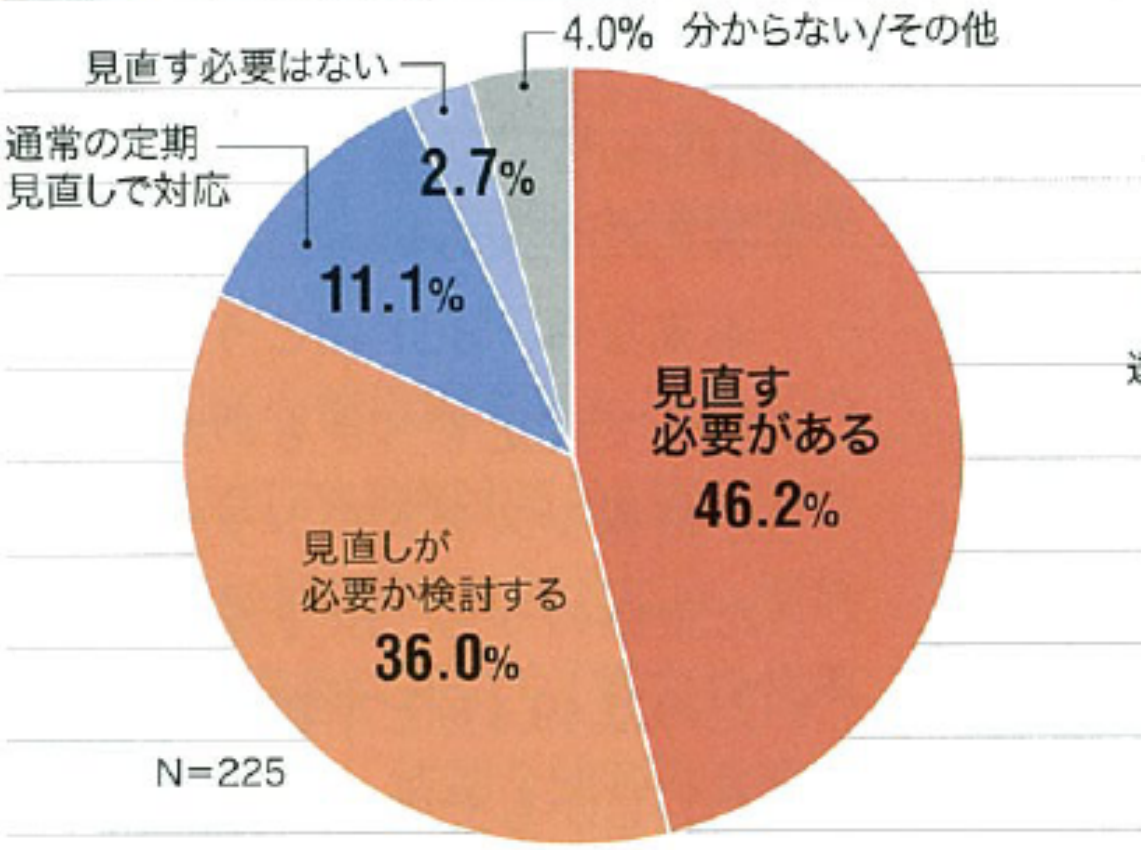


（複数回答）

2010年度までに事業継続計画（BCP）を策定済みの企業は35.9%、2011年度に策定する予定と答えた企業も7.4%と、半数以上の企業はまだBCPの策定に至っていない。

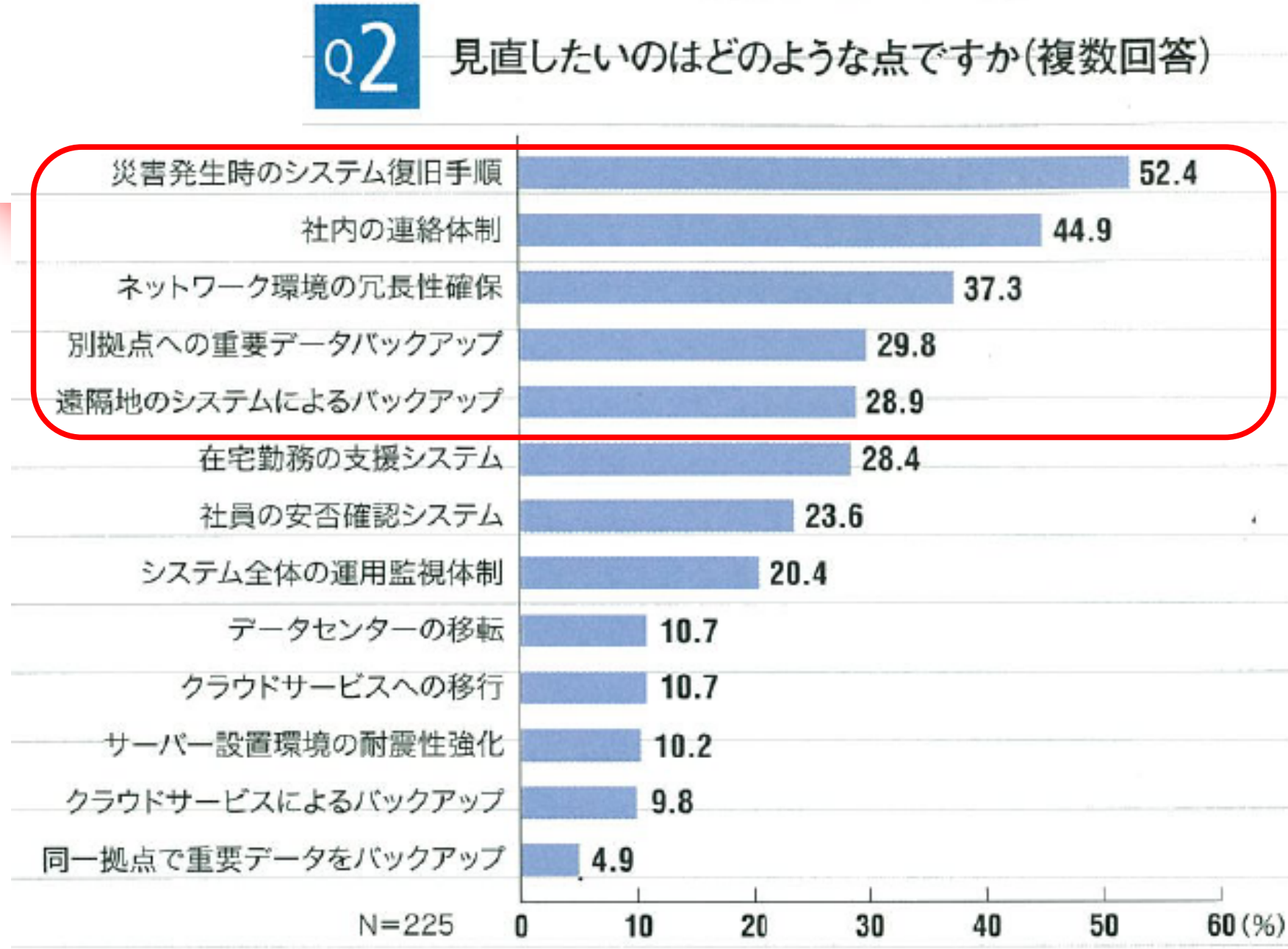
今回の震災を受け、災害時の事業継続のために情報システムに必要と感じた対策を尋ねた結果だ。実際の災害を経験した結果、「非常時における行動ルールやマニュアル類の見直し・作成」が必要と感じた企業が54.8%と過半数を超えた。予想をはるかに超える被害をもたらした東日本大震災を受け、これまでのマニュアルでは不十分だと感じた企業が大半を占めたようだ。

Q1 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があると思いますか(一つだけ)



●調査概要

調査対象:「日経コミュニケーション」読者モニター/調査方法:日経BPコンサルティングのインターネット調査システムで実施/調査日程:2011年3月30日～4月5日/回答企業数(回収率):414社中225社(54.3%)



2011年7月20日発行　ITで実現する震災･省電力BCP完全ガイド　掲載アンケート記事より抜粋

BCPとシステム監査

(組織体が情報システムにまつわるリスクに対するコントロールを適切に整備･運用する目的)

- 情報システムが、組織体の**経営方針及び戦略目標の実現に貢献**するため
- 情報システムが、組織体の**目的を実現するように安全、有効かつ効率的に機能**するため
- 情報システムが、**内部又は外部に報告する情報の信頼性を保つように機能**するため
- 情報システムが、**関連法令、契約又は内部規程等に準拠**するようにするため

BCPとシステム監査
(システム管理基準における事業継続計画)

Ⅰ.情報戦略　－　5.事業継続計画

ICT部門に限定

(1) 情報システムに関連した事業継続の方針を策定すること。
(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。
(3) 事業継続計画は、従業員の教育訓練の方針を明確にすること。
(4) 事業継続計画は、関係各部に周知徹底すること。
(5) 事業継続計画は、必要に応じて見直すこと。

Ⅵ.共通業務　－　7.災害対策

7.1 リスク分析

(1) 地震等のリスク及び情報システムに与える影響範囲を明確にすること。
(2) 情報システムの停止等により組織体が被る損失を分析すること。
(3) 業務の回復許容時間及び回復優先順位を定めること。

7.2 災害時対応計画

ICT部門に限定

(1) リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。
(2) 災害時対応計画は、**組織体の長が承認**すること。
(3) 災害時対応計画の**実現可能性を確認**すること。
(4) 災害時対応計画は、**従業員の教育訓練**の方針を明確にすること。
(5) 災害時対応計画は、関係各部に周知徹底すること。
(6) 災害時対応計画は、必要に応じて見直すこと。

7.3 バックアップ

(1) 情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。
(2) 運用の責任者は、バックアップ方法及び手順を検証すること。

BCPとシステム監査
(システム管理基準における事業継続計画)

Ⅳ.運用業務

－ 4.データ管理

ヒアリング
ドキュメント
現地視察
にて確認

(1) **データ管理ルール**を定め、遵守すること。
(5) **データのバックアップ**の範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。
(8) **データの保管、複写及び廃棄**は、誤謬防止、不正防止及び機密保護の対策を講じること。

－ 6.ソフトウェア管理

(4) **ソフトウェアのバックアップ**の範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。

－ 7.ハードウェア管理

(2) ハードウェアは、**想定されるリスクに対応できる環境に設置する**こと。

－ 8.ネットワーク管理

(4) ネットワークは、**障害対策**を講じること。

－ 9.構成管理

(1) **管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理する**こと。

現地視察
にて確認

－ 10.建物・関連設備管理

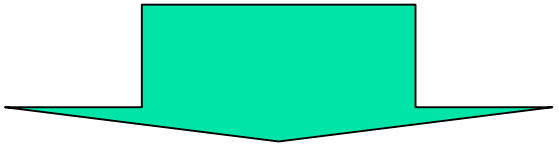
(1) 建物及び**関連設備は、想定されるリスクに対応できる環境に設置する**こと。
(2) **建物及び室への入退の管理**は、不正防止及び機密保護の対策を講じること。
(3) 関連設備は、**適切な運用**を行うこと。
(4) 関連設備は、**定期的に保守**を行うこと。
(5) 関連設備は、**障害対策を講じる**こと。
(6) 建物及び室への**入退の管理を記録し、定期的に分析**すること。

BCPとシステム監査
(システム管理基準における事業継続計画)

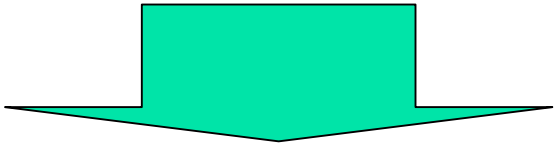
VI.共通業務　－　1.ドキュメント管理

1.1 作成 (5)

(1) ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。
(2) ドキュメント作成ルールを定め、遵守すること。
(3) ドキュメントの作成計画を策定すること。
(4) ドキュメントの種類、目的、作成方法等を明確にすること。
(5) ドキュメントは、作成計画に基づいて作成すること。



重要業務システムごとに未整備部分を見直しして再度整備
(サポートベンダーの協力)



重要業務システムごとに事業継続の方針を作成
(情報システム監査実践マニュアル第2版　付録の様式を活用)

ドキュメント整備支援を通じての協議事項（課題認識事項）等

- ICT部門のBCPだけでなく全社的なBCPに発展させるためには・・・
- 支払い事務に関する業務継続性の検討・・・
- システム運用面のインシデント管理と対応状況について・・・
  （新たな改善テーマの認識と検討）
- 災害発生時のサポートベンダ各社の対応について・・・
- 事業継続性を高めるための取組み項目について・・・

目標に対する評価
(・・・取組み継続中・・・)

1．研究会メンバとしてＢＣＰに関する知識と理解を深める。

「BCAOのステップアップ･ガイド」、「地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン」や参考図書などにより、WGメンバ相互で理解を深めることは出来てきている。

2．ITのビジネスリスクやリスク分析について意見交換し見解をまとめる。

A社との共同作業を通じて、BIAやリスク分析の難しさ(特に金額換算)をより一層実感している。そのような中、A社との活動が出来たことは大きな意味がある。

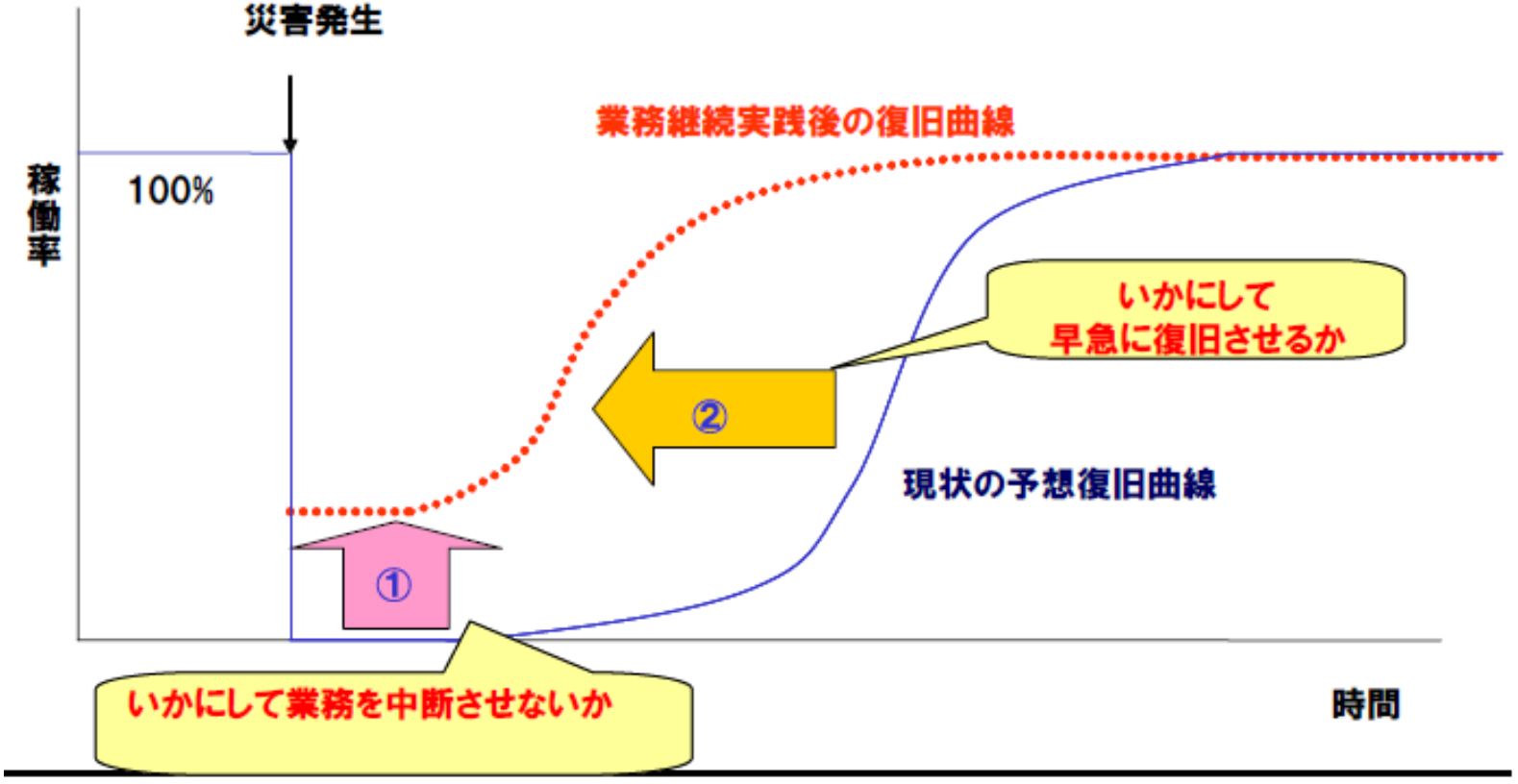
A社の「現状」と「ICT部門の社内的役割」を理解し、「被害想定」という仮説を立て、「リスク対応」を検討し、「経営側の理解」を得て、はじめてICT部門としてのBCPが客観的に認識される･･･。そのための活動を継続中･･･。

3．中小企業にフォーカスしたリスク対応ケースを作る。

「監査部門を持たない」「少ない人員でのIT運営」などの環境にある企業に、「できることから始める」「段階的に進められる」リスク対策ケースをWGで作りたい。

災害や異常発生時に、適切な初動により早期回復･復旧できるIT運営組織の実現。そのための取組みを支援できる研究を継続中･･･。

経営に役立つためのBCP
(早期対処によりビジネス拡大へ)



「地方公共団体におけるICT部門の業務継続計画（ＢＣＰ）策定に関するガイドライン」より抜粋

参考図書やガイドラインなど

- 中小企業ＢＣＰステップアップ･ガイド（NPO 法人事業継続推進機構）
- IT サービス継続ガイドライン（経済産業省）
- 地方公共団体におけるＩＣＴ部門の業務継続計画（ＢＣＰ）策定に関するガイドライン
- 情報システム監査実践マニュアル
- 動かないコンピュータ２０１１
- ビジネスを止めるな　事業継続実践ガイドブック
- 「ＥＲＭで経営を変える－リスクへの戦略的な対応」
- 「ケースで学ぶＥＲＭの実践」
- 「リスクインテリジェンスカンパニー」
- 「安全とリスクのおはなし」
- ISO31000：2009　リスクマネジメント　解説と適用ガイド　　など