BCP研究プロジェクト2014年度活動報告

IT部門の初動対応をモデルとした演習の紹介

SAAJ 西日本支部合同研究会

2014年11月29日 (土)

BCP研究プロジェクト　金子　力造

Systems Auditors Association of Japan

NPO日本システム監査人協会　近畿支部

BCP研究プロジェクト概要

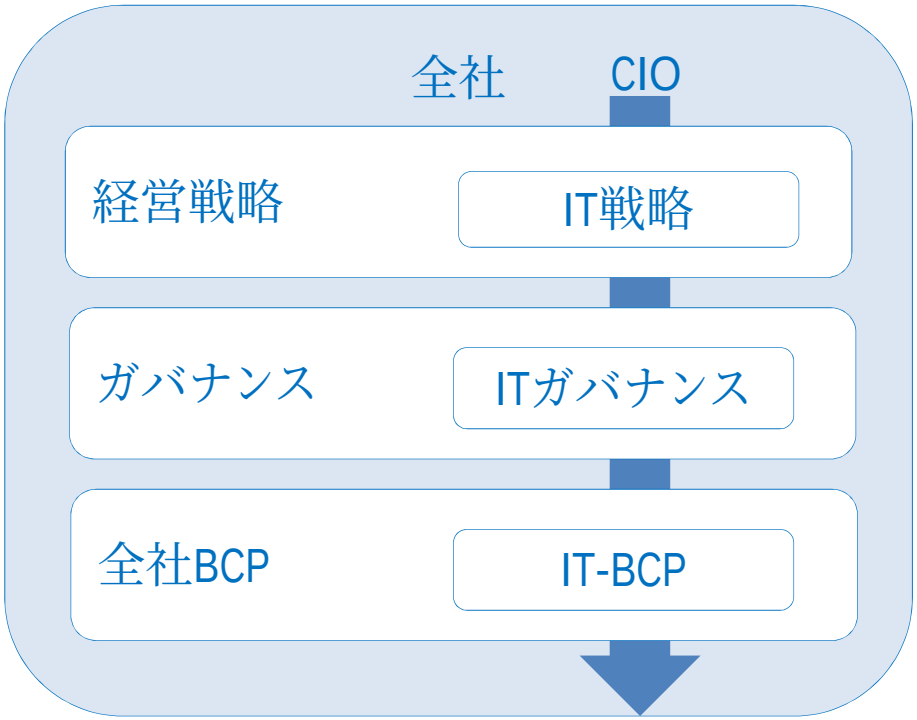
- プロジェクト目標
  - 企業におけるBCP策定にあたっての課題等についてシステム監査人として検討する
  - IT-BCPに関する監査基準･ポイントを整理し作成する
- プロジェクトメンバー（敬称略　５０音順）
  - 荒町弘【主査】、松井秀雄【副主査】
  - 尾浦俊行、川端純一、金子力造、浜田恒彰、吉田博一、和田好文
- プロジェクト活動履歴
  - 2010年～発足、研究会としてスタート
  - 2010年～2011年、某社IT部門に対するBCP策定支援
  - 2012年、BCP策定を容易にする情報システムの検討
  - 2013年、IT部門初動対応と監査ポイントについて検討

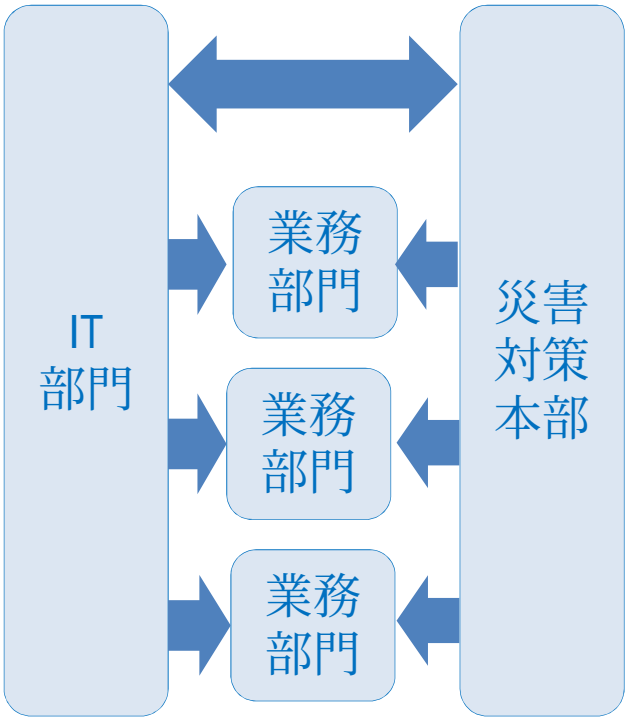
2011年SAAJ研究大会にて

- BCP研究会発表に対するコメント
  - まず全社BCPであり、ITだけ取り出して議論するのは如何なものか？
  - IT部門だけに限定したWG活動としているが、実際には他部門も関係するので、システム監査としての制限はあると思うが、できるだけ他部門も巻き込むような取組みが望まれる。
  - 企業にはBCP策定義務があるのかとの論点があり、会社によっては内部統制構築義務からの要求事項と捉えられる場合がある。その場合には特定部門ではなく全社的に取り組むべき事項である。

IT-BCPとは？

- 事業継続計画の情報システムの復旧について書かれた部分をより詳細化した計画である。
  - 内閣官房情報セキュリティセンター「IT-BCP 策定モデル」より
- IT サービスの継続性を確保することは、必ずしも事業継続性を全て担保するものではない。
  - （経済産業省「IT サービス継続ガイドライン」より）





内閣官房:情報システム運用継続計画より

- 内閣官房情報セキュリティセンター
- 「IT-BCP 策定モデル」（平成25 年6 月版）より抜粋
  - 正式な名称は「情報システム運用継続計画」である。
  - 事業継続計画の情報システムの復旧について書かれた部分をより詳細化した計画である。
  - 災害や事故等の非常時に情報システムを早期に復旧させ継続して利用するために必要な非常時の行動手順で構成される計画である。
  - IT-BCP には、非常時に適切な対応を取るために必要な事前対策や教育訓練等の平常における実施計画が含まれる。

（参照元）http://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf

経済産業省：IT サービス継続より

- 経済産業省
- 「IT サービス継続ガイドライン」（平成24年改訂版）より抜粋
  - 「事業継続計画（BCP）策定ガイドライン」は、計画策定といったいわば高次の内容に焦点を絞っていることから、**IT の現場の立場から見た場合**、同ガイドラインを使用することで高度な事業継続のための対策を直ちに策定できるとは限らないという一面があった。
  - 東日本大震災においては策定していたものの十分ではなかったとの意見もある他、前述したIT への依存性の増大もあり、**事業継続の阻害要因としてIT 関連のトラブル**を挙げる企業の数は非常に多い。
  - IT 依存関係の増加傾向を勘案すれば、**事業継続マネジメント（BCM）の中からIT の要素を取り出して**、IT サービスのマネジメント体制を事故前提の考え方に基づいて構築・維持していくことは、これからの安心・安全な社会の実現にとって必要不可欠である。
  - 本ガイドラインは、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。

（参照元）http://www.meti.go.jp/policy/netsecurity/docs/secgov/2011_IoformationSecurityServiceManagementGuidelineKaiteiban.pdf

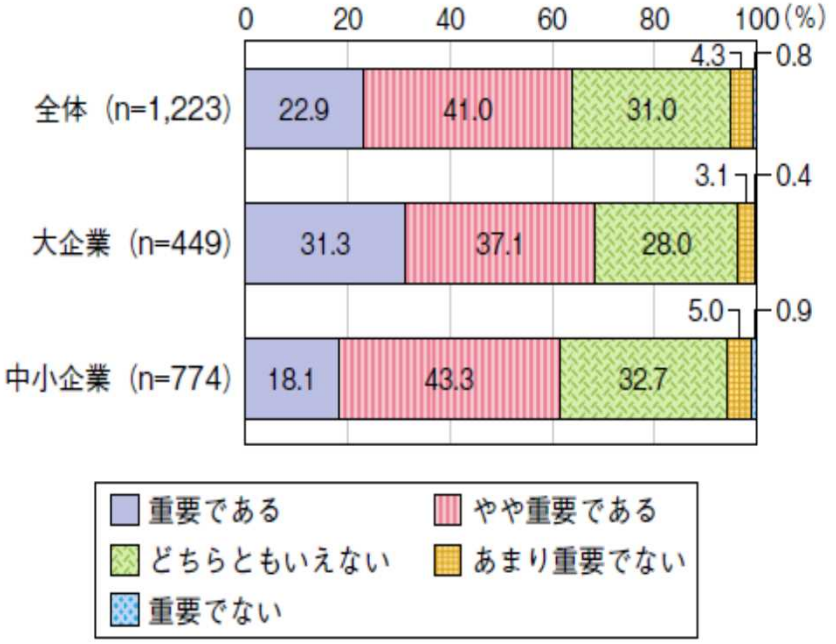
総務省：ICT部門の業務継続計画より

- 総務省
- 「ICT部門の業務継続計画＜初動版解説書＞」（平成25年5月版）より抜粋
  - 特に業務のIT依存度が高い今日においては、ICTは重要なインフラの一つであり、災害時においても、**ICT資源を活用できるか如何がその後の復旧・復興活動に大きく影響する**ことが考えられる。
  - 全庁的なBCPの策定がすぐには行えない場合でも、**初動部分のICT-BCPだけでも先行して策定することは可能**であり、また、ICT-BCPを先行することで活用できるICT資源が明確になり、全庁のBCP検討がし易くなる面もある。
  - いきなり100％のものを完成させる事を考えずとも、解説書の手順等を参考に、まずは取組むことが重要であり、**早めに訓練を行って問題の認識を高めてから改善していく**など、PDCAサイクルの中で完成度をあげていくやり方もあると思われる。

（参照元）http://www.soumu.go.jp/main_content/000222227.pdf

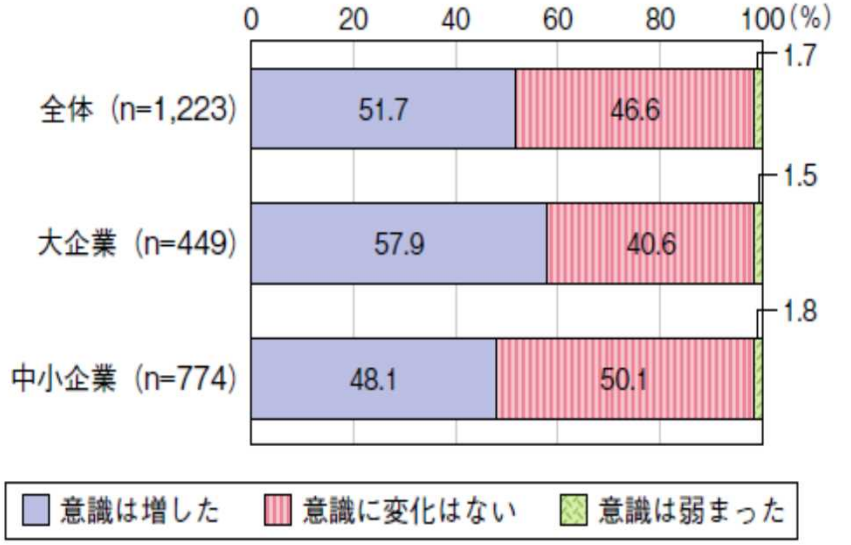
IT-BCPへの意識の変化

図表 3-2-3-2 業務継続計画（BCP）におけるICTの重要性 （民間）



（出典）総務省「ICTが成長に与える効果に関する調査」（平成24年）

図表 3-2-3-3 東日本大震災を契機とした業務継続計画(BCP)におけるICTの重要性意識の変化 （民間）



（出典）総務省「ICTが成長に与える効果に関する調査」（平成24年）

平成24年度 情報通信白書より

東日本大震災後に、ICTの重要性の意識は高まったが、
それでもIT-BCP策定が進まない．．

大企業におけるIT-BCPの策定状況

- プライスウォーターハウスクーパース株式会社
- 「IT- BCPサーベイ2014」の調査結果より抜粋
- 国内の上場企業及び有力未上場企業（有効回答数：131社）
  - 回答企業の約4割は、IT-BCPを定めていない。
  - 情報システムの中断・停止に備えた訓練・演習を行ったことがない企業は、回答企業の約4割にのぼる。
  - IT-BCP対応予算の割合は、情報システムの予算のうち1%以下と回答した企業が、約5割を占める。
  - 重要業務の継続／早期復旧に必要となる情報システムをすべて特定できている企業は、回答企業の約3割にとどまる。
  - 情報システムの復旧優先順位を経営陣が最終決定している企業は、回答企業の約2割にとどまる。
  - 回答企業の約6割は、バックアップサイトを保有・契約していない。
  - データセンターの約3割においては、電力会社からの送電が24時間停止してしまうと、稼働停止してしまう。

（参照元）http://www.pwc.com/jp/ja/advisory/research-insights-report/it-bcp-survey2014.jhtml

なぜ今IT-BCPなのか？

ITT-BCPの必要性

- 今日ITは、事業継続に必須の経営資源として重要性が増大している。
- 今日ITは、コア業務のみだけでなく社内の全業務と関係している。
- 東日本大震災の教訓から、初動のスピードと的確さが復旧に大きく影響するという認識が高まった。
- 東日本大震災の教訓から、IT資源の喪失により初動対応が十分にできず、その後の復旧、復興に大きく影響する事態が発生した。

ITT-BCPが普及しない理由

- IT担当としての悩み。
- 何から始めればよいか分からない。
- トップの理解が得られない。投資効果がわかりにくい。
- そもそもITは、後回しにされている。

どうすればIT-BCPは普及する？

- 企業活動に不可欠なITインフラとしての認識を高める。
- IT-BCPが企業の競争力につながることの理解促進。
- IT-BCPの必要性の啓蒙する。

IT-BCPの普及のためには、まず取り組むための動機「気づき」が必要なのでは？

IT-BCP体験セミナーを企画

IT-BCPに取り組む入門編として

IT-BCPの重要性は理解できても、策定に着手するにあたってどのように取り組むべきか？「ノウハウが無い」「時間が無い」「必要性の理解が得られない」など様々な懸念があります。

ケースシナリオを使った体験演習を通じてIT-BCPの必要性を理解し、ポイントを学んでもらう

1. 初動対応の演習を通じて、IT部門はいざという時どのような行動が要求されるのか**体験**する。
2. グループ討議での気づきをもとに、IT-BCPの重要性と自社で取り組む場合のポイントを**確認**する。
3. IT-BCP策定への道筋として、災害対策本部運営の実際や訓練・演習で鍛えるIT-BCPについて**学ぶ**。

IT-BCP体験セミナー半日コースをセミナーWGの協力により2014年10月25日(土)に開催した

IT-BCP体験セミナーの概要

巨大地震が発生！あなたはどう行動しますか？

- IT-BCP体験セミナー半日コース
  - 【開催】2014年10月25日(土)13:00 ～17:00
  - 【会場】大阪大学中之島センター
  - 【参加】10名

- 演習のケースシナリオ
  - 舞台：近畿圏に30店舗のスーパーを営む従業員数1800人の会社
  - 災害：南海沖で地震発生！本社（大阪）震度5強
  - 貴方：システム課の課員

その時、IT部門はどうする？ あなたは何をする？

- BCP研究プロジェクトで、今まで検討してしてきた内容をシナリオに盛り込む。さらに演習の後の講義で理解を深める。

IT-BCP体験セミナーの構成

体験と講義から「自社もやらなければ！」という動機と取り組むヒントに繋げる

- カリキュラム
- 【演習】災害発生直後の初動対応演習
  - 初動対応の演習を通じて、IT部門はいざという時どのような判断が要求されるのか体験しグループ討議での気づきをもとにIT-BCPの重要性とポイントについて学びます。
- 【講義】危機対策本部の実際　(講師：尾浦俊行氏)
  - 過去の大規模災害等における自治体の対策本部の実際を紹介しながら、BCPの発動から、本部設置、活動継続における実効性向上について提言します。
- 【講義】訓練・演習で鍛える IT-BCP　(講師：松井秀雄氏)
  - IT-BCP 訓練・演習の実施状況から、某社での実機を使った訓練の紹介、有効な机上訓練のやり方としてIT版DIG(*)の実践を提言します。 (*)DIG・・・災害図上訓練の一手法 (DisasterImaginationGame)

初動対応演習の内容と報告

カリキュラム

- 事例企業の解説（20分）
- 演習１「災害発生直後の初動対応」
  - グループ演習と発表（30分）
- 演習２「IT-BCPのポイント検討」
  - グループ演習と発表（40分）

ケース企業A社概要

社名	A社
事業内容	近畿圏に30店舗のスーパーを営む
取り扱い品目	精肉、水産、青果、食品、総菜、日用品、雑貨、酒、薬品など
所在地	本社（中央区堺筋本町）鉄筋5階建自社ビル 店舗（北大阪地区、南大阪地区、東大阪地区、神戸地区、和歌山地区） 倉庫（南港） データセンター（三田市）Dデータセンターのハウジングサービスを利用
売上	年間800億円
従業員数	1800人（内正社員は300名）

A社のBCP導入の経緯と現状

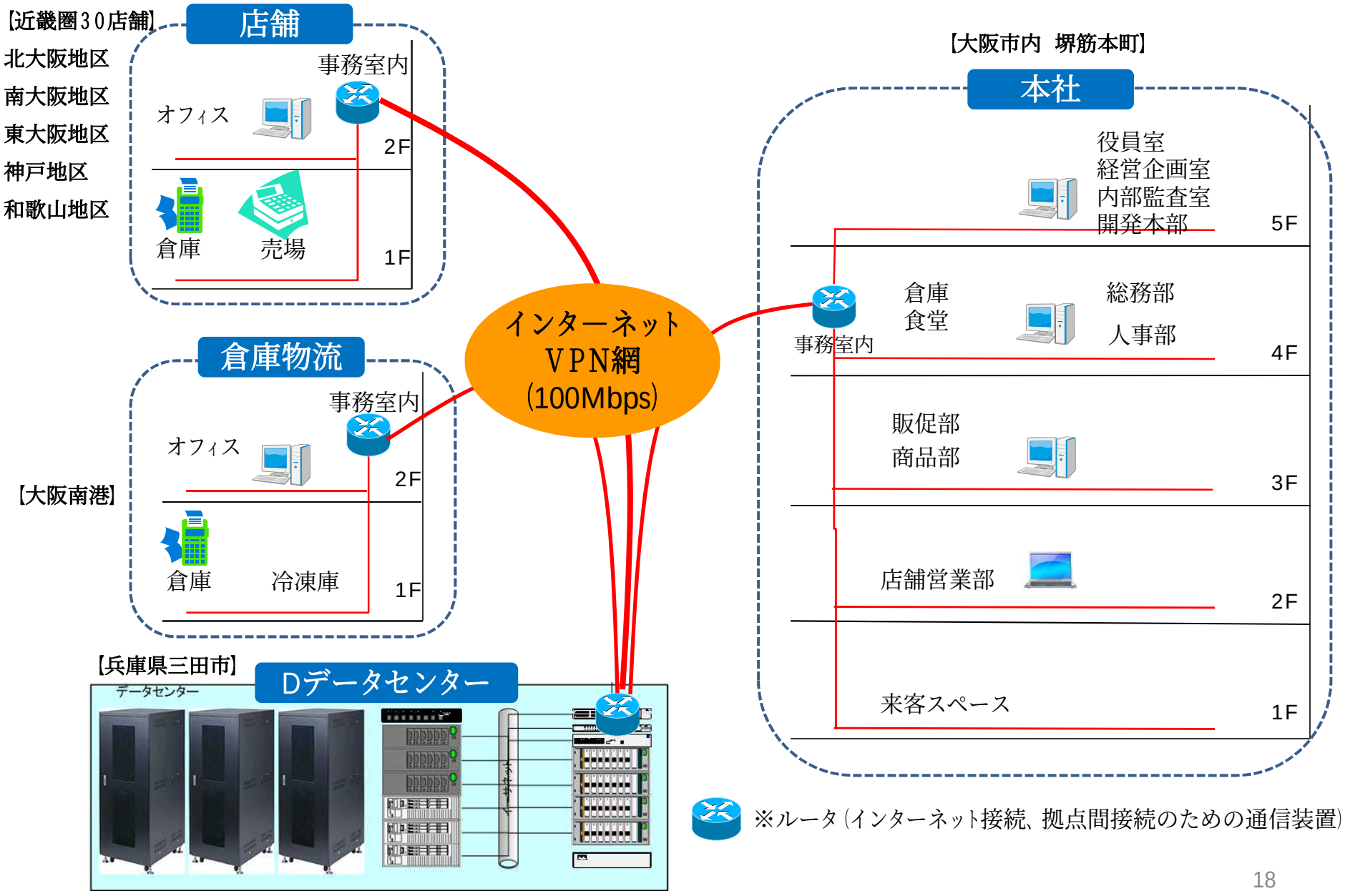
- BCPの導入状況
  - A社は、近畿圏に30店舗のスーパーを営む会社である。生活必需品の供給（食料、日用雑貨）行っていることから災害時における地域での責務も大きい。自治体からの意向もあり、1年前からBCP策定に取り組んでいる最中である。
- IT-BCPの状況
  - 重要業務に関連する販売管理システムなどの情報システムをデータセンターに預けていることで一定の業務継続が保証されているものと考えている。経営幹部のITに対する理解は低く、ITについて自主的な復旧計画等を策定することの必要性は認識していない。

A社主要システム一覧

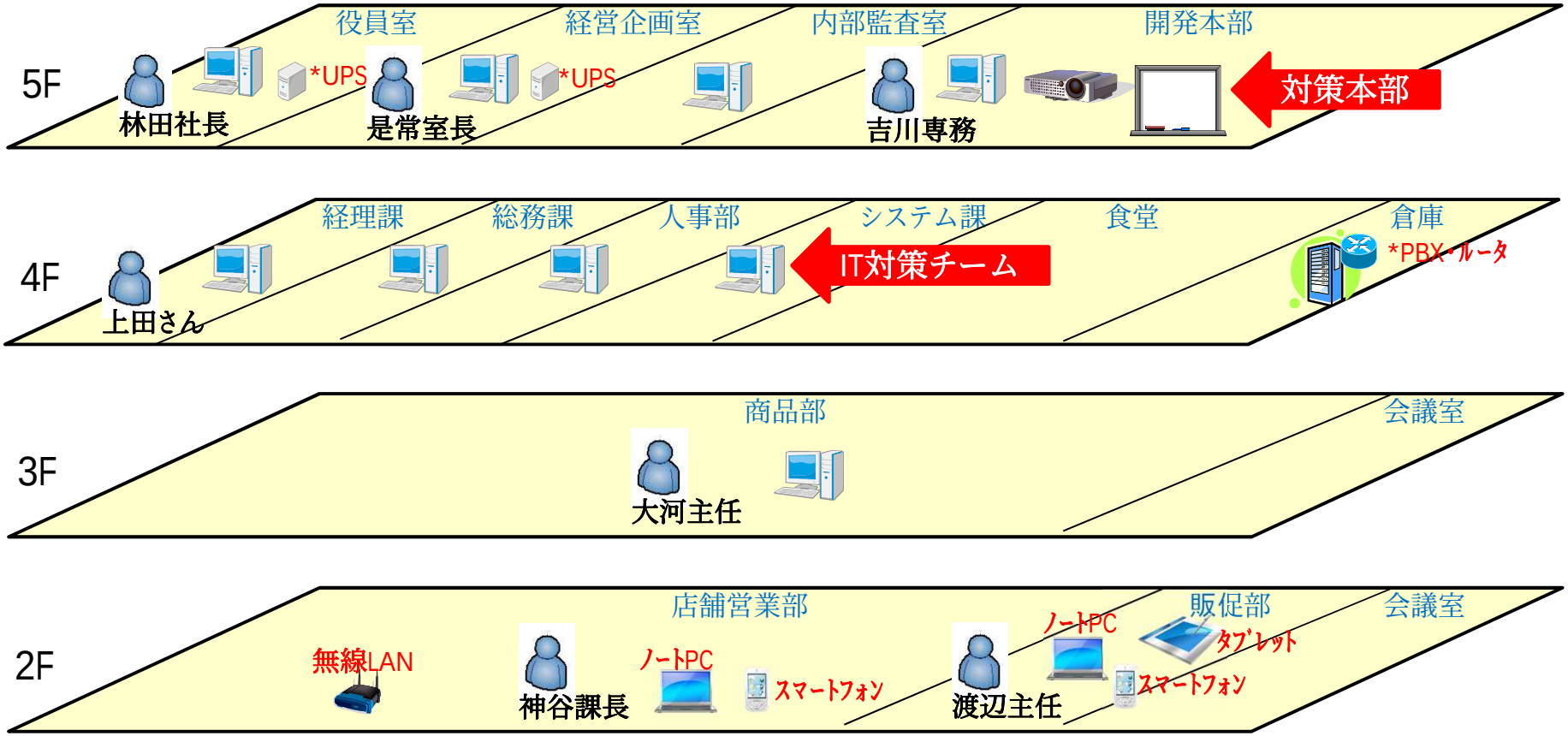
システム名	用途、内容	形態	所在	主な利用者
販売管理システム*	商品の発注から仕入れ、販売、棚卸しを管理するシステム。POSレジシステムや在庫管理用のハンディターミナルと連携している。	ﾊﾟｯｹｰｼﾞ カスタマイズ	Dﾃﾞｰﾀ ｾﾝﾀｰ	営業本部 店舗
POSレジシステム*	バーコードスキャナーを設け、商品を読み取る事により単品単位で販売時点情報を管理すると共に、レジ打ち作業のできる端末。WindowsをOSとして動作している。ストアーサーバと連携している。	ﾊﾟｯｹｰｼﾞ	店舗	店舗
ハンディターミナル*	バーコードスキャナーを設け、倉庫や店舗のバックヤードで、商品の入庫時や棚卸し時に、商品のバーコードを読み取って販売管理システムにデータ転送するための端末。売上の登録もできる。	ﾊﾟｯｹｰｼﾞ	店舗	店舗
倉庫物流システム	一括仕入した商品を保管している倉庫で、商品の保管管理のために使用しているシステム。販売管理システムと連携している。	ﾊﾟｯｹｰｼﾞ	Dﾃﾞｰﾀ ｾﾝﾀｰ	商品部 倉庫
EDIシステム	一部のメーカーとの電子商取引のために使用しているシステム。	ｵﾝﾗｲﾝ	取引先	商品部
財務会計システム	財務、会計を管理。スタンドアロンで使用している。	ﾊﾟｯｹｰｼﾞ	本社	経理課
支払い業務システム（インターネットバンキング）*	取引先への支払いや従業員の賃金払い等のために使用する銀行とのオンライン通信システム。	ｵﾝﾗｲﾝ	本社	経理課
勤怠システム	従業員の勤務管理を行うシステム。スタンドアロンで使用している。	ﾊﾟｯｹｰｼﾞ	本社	人事課
給与システム	従業員の賃金計算のために使用しているスタンドアロンシステム	ﾊﾟｯｹｰｼﾞ	本社	経理課
グループウエア	メール、掲示板、文書管理、電子会議室、ワークフローなどの機能を備えており自社で独自システムを作成することが可能である。	ﾊﾟｯｹｰｼﾞ カスタマイズ	Dﾃﾞｰﾀ ｾﾝﾀｰ	全社員
ファイルサーバ	部門毎にアクセス権を設定したフォルダを作成し、部門の業務に必要なファイルを保管している。		Dﾃﾞｰﾀ ｾﾝﾀｰ	全社員
安否確認システム*	全社ＢＣＰ策定時に、セキュリティ会社Ｓ社とサービス利用の契約をした。	WEBｻｰﾋﾞｽ	Ｓ社ｾﾝﾀｰ	全社員

*印・・・重要度の高いシステム

A社事業所配置


【近畿圏30店舗】
北大阪地区
南大阪地区
東大阪地区
神戸地区
和歌山地区
店舗
事務室内
オフィス
2F
倉庫
売場
1F
【大阪南港】
倉庫物流
事務室内
オフィス
2F
倉庫
冷凍庫
1F
【兵庫県三田市】
Dデータセンター
データセンター
インターネット
VPN網
(100Mbps)
【大阪市内　堺筋本町】
本社
役員室
経営企画室
内部監査室
開発本部
5F
事務室内
倉庫
食堂
総務部
人事部
4F
販促部
商品部
3F
店舗営業部
2F
来客スペース
1F
※ルータ（インターネット接続、拠点間接続のための通信装置）

A社本社フロア別･部署別情報



【IT端末･情報機器類】

*UPS･･･突発的な停電や電力障害に対し一定時間電力を供給し、安全に停止するための電源装置。
*PBX･･･構内の電話回線を集約し、外線(公衆回線)との接続、切り替えや内線通話できるようする装置。
*ルータ･･･インターネット接続、拠点間接続のための通信装置。

災害発生とA社被害の状況

災害の規模と地域の被害

- 6月20日（金）午後13:00南海沖で地震発生。
- 本社（大阪）震度5強。和歌山震度6。
- 大阪市内で一部停電。交通機関は一部マヒしている模様。

本社（堺筋本町）の状況

- 建物は、倒壊せず軽微な損傷。エレベータは、停電で使用出来ない。
- 建物に発電機等非常用電源はない。
- パソコン等を含む機器等は、落下転倒等で多数破損している。
- 倉庫内の荷物が崩れて、中に入れない状況である。

＜通信設備＞

- 通信設備は、倉庫内の専用ﾗｯｸに収納されており、非常用電源は無い。
- 固定電話やFAXは、停電で使えない状況となっている。内線も使えない。
- 携帯の通話は繋がりにくい状況、メール、ショートメールは使える。

倉庫（南港）

- 余震により津波の恐れがある。

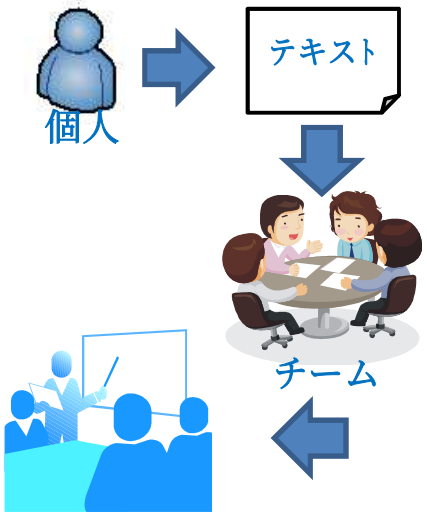
データセンター（三田）

- 軽微な損害で通常サービスを継続している。

演習の進め方

個人での検討と、チームでの討議

1. 各自シナリオの状況説明を読み対応案をテキストに記載する。
2. それぞれの案をもとに、チームで最適な対応案を討議、検討する。
3. 意思決定した内容を模造紙に記入しチーム発表。

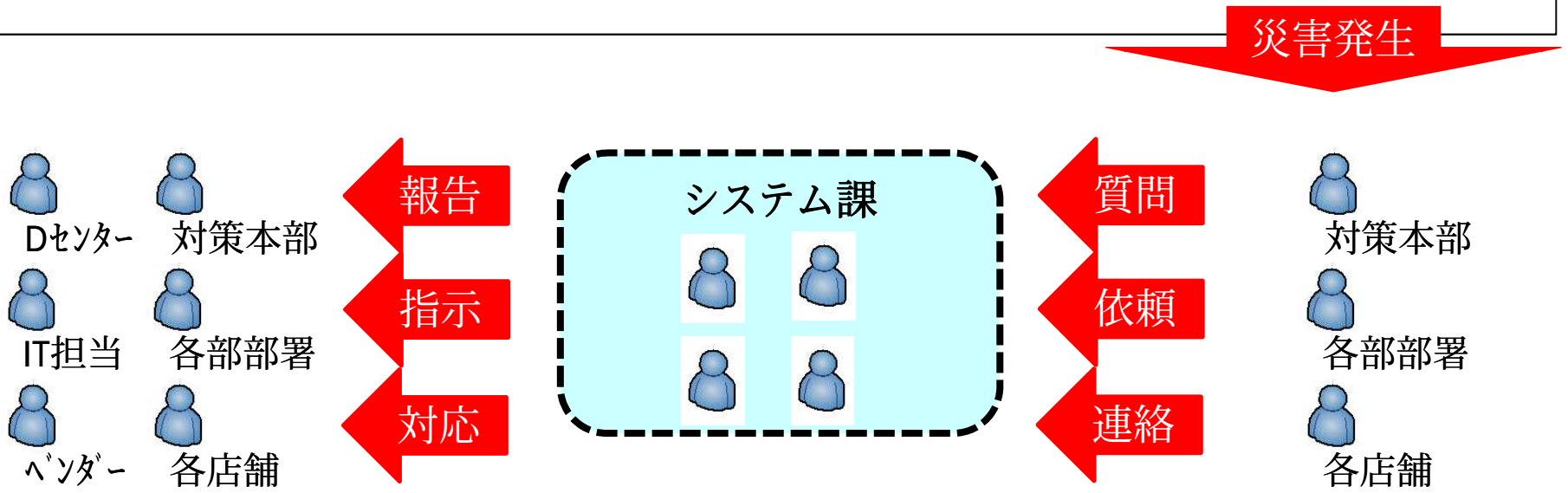


演習のポイント

- 時間配分を考え、短時間で意思決定する。
- それぞれのリクエストに対する優先順位を、緊急度や重要度の観点から検討する。
- 可能な限り自ら対処するのではなく、どの部署の誰にどのような指示を出すかを検討する。

演習1：IT部門の初動対応体験

- チームのミッション（貴方の役割）
  - システム課は、この緊急時に対策本部の下、IT対策を担うことになった。各部署及び各店舗からの様々な問い合わせ、依頼要求が来る。限られた時間内で意思決定し、指示出しを行うこと。



Scene00. (状況サンプル)

- 商品部大河主任から報告
  - 「そこら中のPCが机の上から落ちて、大変なことになっています！！どうしたらいいですか？」

Point

IT機器の大規模な被害に対し初動でどう対応する？

- Action ー貴方ならどうする？チームはどの様に判断し対処すべきか？

？

9つの状況（Scene）を解決する

＜＜演習の風景＞＞




• Scene01 • 対策本部の吉川専務から – ○○○が、使えないけど. .	• Scene02 • 店舗営業部の神谷課長から – ○○○は、どうなってるんだ！	• Scene03 • 経理課の上田さんから – ○○○が間に合いません！
• Scene04 • 林田社長から – ○○○すぐ来い！	• Scene05 • 対策本部の吉川専務から – ○○○報告してくれ！	• Scene06 • 和歌山店の鈴木店長から – ○○○どうしたらいいですか？
• Scene07 • 経営企画室の是常室長から – ○○○してもいいかな？	• Scene08 • 堺店の中村店長から – ○○○という状況です！	• Scene09 • 対策本部の吉川専務から – ○○○今日中に頼む

演習2：IT-BCPのポイント検討

- チームのミッション
  - システム課では、今回の体験によりBCPだけでは、社内ITの危機対応が難しいことを認識した。チームで今回の体験を踏まえ、IT-BCPの策定に向けて、それぞれの課題ごとに下記のポイントを討議する。

  - 事前に決めておけばよい行動計画やルールは？
  - 危機対応時にあれば役に立つ文書や資料は？
  - ダメージを少なくする事前の対策は？

システム課は、討議内容をまとめ対策本部に報告提言する

Scene00. (課題サンプル)

- 商品部大河主任から報告
  - 「そこら中のPCが机の上から落ちて、大変なことになっています！！どうしたらいいですか？」

Point

クライアントＰＣの重要度は認識しているか？

事前に決めておけば良かった行動計画やルールは？	危機対応時にあれば役に立つ文書や資料は？	ダメージを少なくする事前の対策は？
？	？	？

受講生された方の感想

- セミナーの満足度（参加者10名中）
  - 期待以上（1名）、期待どおり（4名）、ほぼ期待通り（5名）
- アンケートより抜粋
  - 演習を通じて、様々な気付きが得られました。
  - 実践形式がよかった。聞くだけではなかなか分からない。
  - 演習により、5W1H、特に誰が、という指示の重要性等気づきがあり参考になりました。
  - ダラダラとしている時間は無いという感覚が身体で分かった。
  - 初動時に考えることがイメージできました。
  - 頭の中には一般的なBCPが入っているのですが、ITに特化した初動が分かってきたような気がする。
  - 演習、実践のヒント、盛りだくさんで、使っていける手法を一つ一つ試していきたいと思います。
  - BCP、IT-BCPについて、自社の対応を考えるのに役立つ内容でした。

実践形式による演習の評価は高い！

演習の方法について

- **初動対応の体験（意思決定の演習）**
  - 足りない時間、足りない資料、不十分な説明、意味不明のリクエスト、スキルもバラバラで何が出来るのか？
  - 実際の危機対応時には、もっと余裕ありますか？

インバスケット演習

- 目的は**気づき**
- **動機づけと課題の認識**
- **限られた時間**で多数の案件を一度に処理し意思決定する。

図上訓練

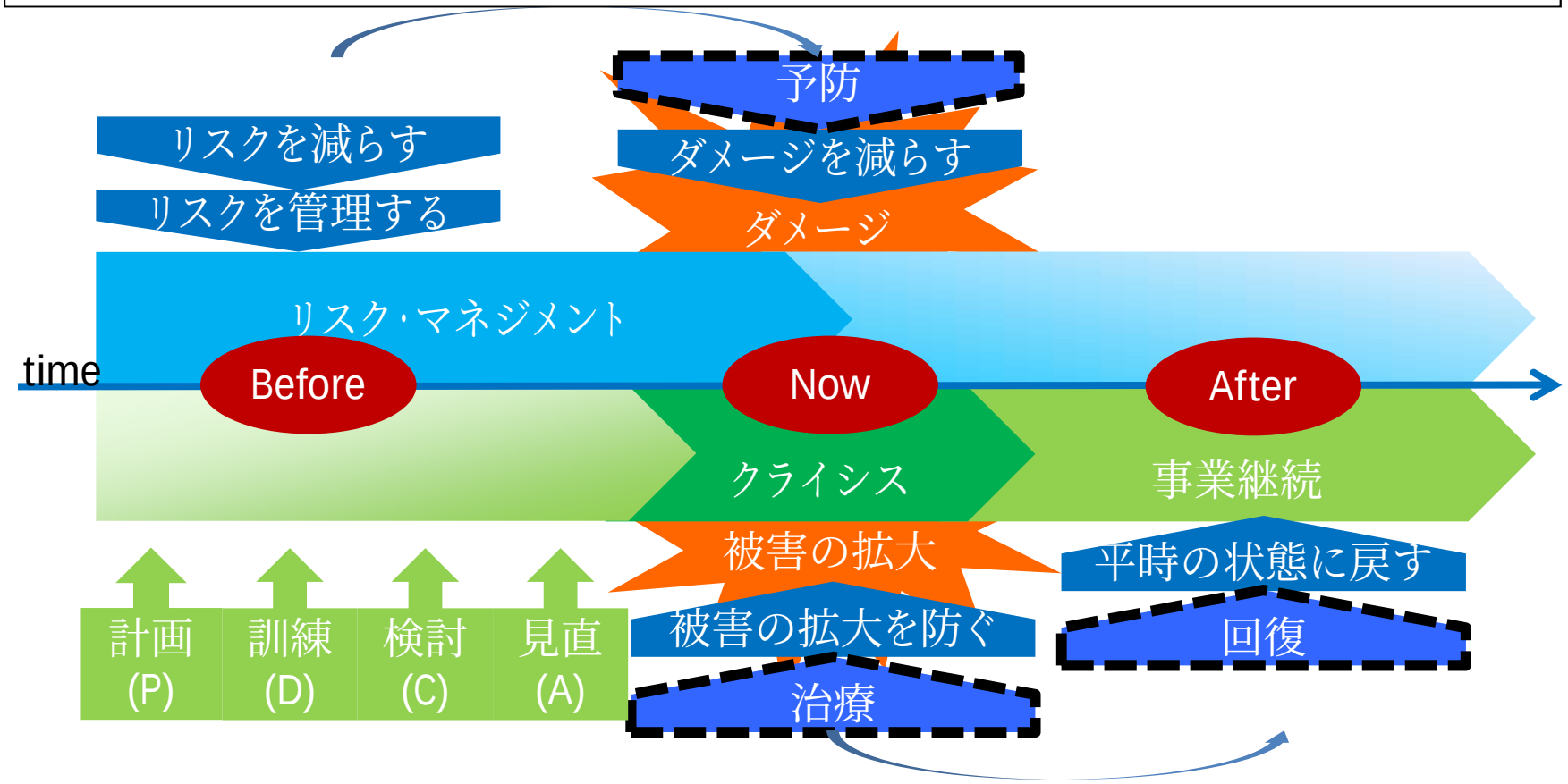
- 目的は**訓練**
- **危機対応力**の強化
- **リアルタイム**に事態が進行する中で危機に対応していく。

①分析 問題を **把握する** → ②選択 **優先順位** をつける → ③結論 短時間で **意思決定** → ④実行 **指示出し** コマンド

出来ない人＞＞＞**フリーズ**、場当たり、放置、指示待ち、**先送り**

リスク管理－危機管理－事業継続計画の関係

- リスク管理、危機管理、BCP、防災などの関係
  - 「やること」が重なっている部分が多いため混同されやすい。
  - それぞれ「何の為に？」を時間軸に沿って整理すると、「予防」「治療」「回復」と、重点とする目的が異なる。



BCPはダメージを前提とした回復への道筋。復旧時間が長いほど損失は拡大する

IT部門の初動対応ポイント

対策本部の初動

1. BCP発動フェーズ
   - 本部要員の参集
   - 災害情報の収集
   - BCP発動の判断
2. 本部稼働フェーズ
   - 対策本部の設置
   - 社員安否の確認
   - 被害情報の収集
3. 仮操業フェーズ
   - 業務シフトの決定
   - 復旧方針の決定
   - 情報発信、情報公開

連携

IT部門の初動

1. BCP発動フェーズ
   - 幹部間連絡の手段
   - 災害情報収集の手段
   - ＢＣＰ情報発信の手段
2. 本部稼働フェーズ
   - 本部のICTインフラ準備
   - 安否確認ツールの準備
   - ICT資源被害の調査
3. 仮操業フェーズ
   - ICT復旧要員の確保
   - ICT復旧方針の決定
   - ホームページの更新等

BCP

IT-BCP

初動対応から復旧へ向けての要素

STEP1:対策本部の活動に必要なITを、早急に機能させる

- 災害発生直後の対策本部では、意思決定に必要な下記の3つの情報コントロールが重要となる。
  - 情報収集（災害情報、安否情報、被害情報など）
  - 情報発信（BCP発動、指揮命令、広報情報など）
  - 情報共有（復旧方針、復旧計画、資源配分など）

STEP2:重要業務の仮操業に必要なITを、有効に機能させる

- 初動フェーズでは仮操業へ向けて、資源の再配置を行う。
  - 安否確認結果と業務所掌とのマッピング
  - 重要業務への資源の最適シフト
- IT部門は、上記に関連するICTインフラに責任をもつ。

STEP3：復旧に向けて全業務のITを、円滑に回復させる

では、IT部門は何が出来るのか？何をすべきか？

BCPの構築手順から

実施フロー	ポイント
プロジェクトメンバーの選定	誰がやるの？（＋経営者のサポート）
事業継続方針の決定	何のためのIT-BCP？
対象範囲の絞込	重要なシステムって何？
復旧目標の決定	そのシステムはいつまでに必要？
現状の調査	ドキュメント類はある？
事前対策の検討	Befor：ダメージを少なくするには？
行動計画の検討	After：その時どう動くのか？
文書化する（BCP）	作るのが目的ではない！
教育・訓練・事前対策の実施	定着させるために、せめて年1回
計画の見直し	古い計画は役に立たない！

教育・訓練の気づきからスタートする方法もあるのでは？

IT-BCP策定へ向けての提言

書式を埋めることが目的になっていませんか？

- BCPは、計画書（ドキュメント）作成が目的ではない。
  - ぶ厚いBCPのファイル本当に使いますか？
  - 100社あれば100通りのポイントがあるはずです。
  - 自社で起こりうるシーンを想像し、自社のシナリオを作成して見てる。また実際に社内演習を行って見る。
  - そこから、自社に本当に必要な実効性のある対策、BCPに必要なITの要素が見えてくるのでは？
  - 本セミナーは、演習を起点とした気づきからBCPへ取り組むためのアプローチとして企画されました。

今後のプロジェクト目標

- 本プロジェクトの最終目標は、策定されたIT-BCPについてシステム監査を行うこと！！
  - その為に、多くの組織でIT-BCPが策定されていなければならない。
  - その為に、多くの人にIT-BCP必要性を理解してもらう必要がある。
  - その為の、実践的な普及セミナーを今後も企画していく予定です。

SAAJ近畿支部のBCP研究プロジェクトでは、
IT-BCPをテーマに毎月1回活動を行っています。

IT-BCPに興味のある方ならどなたでも！

是非ご参加下さい。

問い合わせ先（contact@saajk.org）

BCP研究プロジェクト主査：荒町弘まで

ご清聴ありがとうございました