日本システム監査人協会近畿支部
第１５０回定例研究会

IT-BCPの実効性を高める訓練･演習とその監査

２０１５年１月１６日（金）

公認システム監査人　　松井秀雄

お話の順番

＊ 簡単に自己紹介

1. IT-BCPの実効性を確認・向上する方法は？
2. IT-BCP の訓練・演習の実施状況
3. 実機訓練で得られる気付きと改善
4. 机上訓練で得られる気付きと改善
5. IT-BCPの実効性に関するシステム監査の視点
6. 「想定外」への備えは可能か？

＜こんな設計・テスト・事故・研究会を経験＞

★各種2センター方式
- ・コールドスタンバイ方式
- ・東阪分担方式
- ・ホットスタンバイ方式

★銀行勘定系のタスク構造
- ・ユーザー・サブタスク方式
- ・サブタスク方式
- ・多重アドレス空間方式

★構成要素障害影響分析（CFIA：Component Failure Impact Analysis）

★IT機器（CPUやディスク装置他）の障害回復手順の作成～回復テスト

★基幹業務用CPUやディスク装置の二重化設定～代替テスト

★予期せぬ災害や事故も経験
- ・世田谷電話局火災　　1984年11月16日 正午頃 ⇒ 東阪分担が効果
- ・阪神淡路大震災　　1995年 1月17日 午前5時46分

★全国IBMユーザー研究会の下部組織である関西IT研究会
- ・2007～2008年 「いざという時に役立つBCP」
- ・2011～2012年 「想定外の事態に備えるBCP」

1. IT-BCPの実効性を検証・向上するための推奨事項

1.1 ISO での要求事項

事業継続マネジメント ISO22301 ：
策定したBCPの実効性を検証する要求事項として
「8.5 演習およびテスト」

IT-BCMに関する ISO27031 ：
実効性を高める取り組みとして、
「7.5 意識・能力の向上、および訓練プログラム」

1.2 各種ガイドラインでの推奨事項

IT サービス継続ガイドライン・改訂版（経済産業省　平成24年）：

「5.4 テストと監査」の目的　：「IT サービス継続計画の有効性を確認するとともに、IT サービス継続マネジメントが正しく維持されているかを確認するため」

IT-BCPの「有効性」を確認する手段　・・・「テスト」
IT-BCPの「維持」を確認する手段　・・・「監査」

地方公共団体におけるICT部門の事業継続計画(BCP)策定に関するガイドライン　（総務省　平成20年）：

「ステップ7：ICT部門内の簡易訓練」の【必要性】：
策定した初動計画をはじめとした計画が非常時に有効に機能するためには、定期的に訓練を実施して、職員等関係者が計画どおりに行動できるようにすることが必要不可欠である。また、計画の実効性の確認や改善のためにも必要である。

「ステップ16：本格的な訓練の実施」の【必要性】：
「策定した業務継続のための行動計画や事前対策が非常時に有効に機能するためには、定期的に訓練を実施して、職員等関係者が理解を深め、計画どおりに行動できるようにすることが必要不可欠である。
ステップ7で実施した訓練に加えて、より高度な訓練を実施する。

＜参考＞　テストの種類

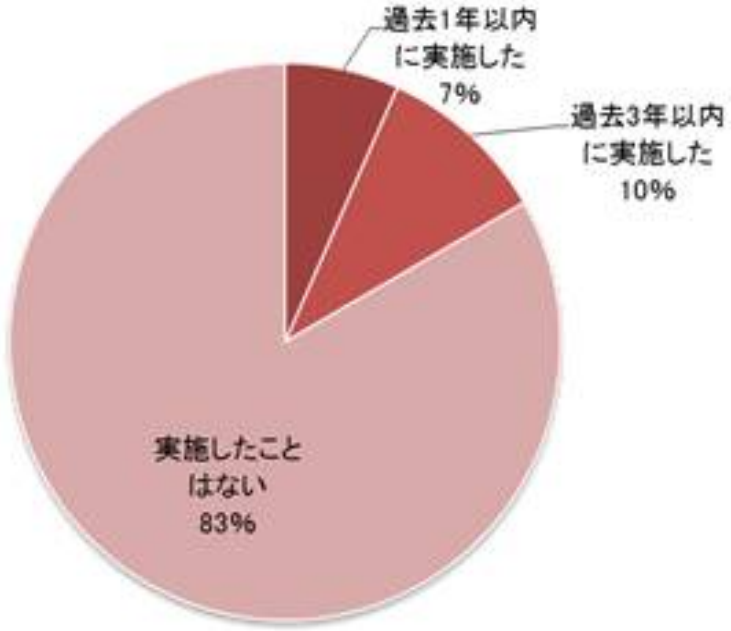
テストの種類	実施内容	メリット	デメリット
机上チェック	・計画の内容をレビュし、 不具合を修正する ・計画に定めた各種内容の 有効性を検証する	早期に実施可能であり、 事業への影響が少ない。 必要要員も最少である。	対応能力の向上や 対応手順の良否の 検証は難しい
ウォークスルー	・計画に定めた各種内容の 有効性を検証する	早期に実施可能であり、 事業への影響が少ない。 必要要員も最少である。 机上チェックよりも、より末端の 対応手順を検証できる。	計画自身の整合性の 検証が中心であり、計画 発動時の具体的な課題提示 は難しい。
シミュレーション	・計画発動時に予想される状況 を前提として、計画の実行に 必要かつ十分な情報が記載されている ことを確認する。	状況を与えることで、より 深い計画の検証を行う。 あらかじ め与えられた状況内であるが、これ に沿って例えば対応チームごと に 対応手順内容を検証できる	必要要員は多くなる。
ロールプレイング	・テスト実施の途中で状況を追加付与し、 参加者の状況判断や 意思決定の可否、連絡体制などを検証 する。	計画を実行する判断者の訓練にな り、判断資料の手当てなどが確認 できる	想定状況を多数設定するため、 事前準備の負荷は大きい。参加 者の十分な知識も必要となる。 必要要員は多い。
実機訓練	・実際の設備などを用いたテスト を実運用及び実作業で行える ことを検証する。	代替施設や設備に関して 実際の手順を適用し、実効性の有 無を確認できる。 代替システム切り替えなど 実際の手順を経験できる。	業務に影響する可能性があり、 周到な準備が必要である。現場 レベルで多数の要員確保も必要 となる。

出典:「IT サービス継続ガイドライン・改訂版　経済産業省

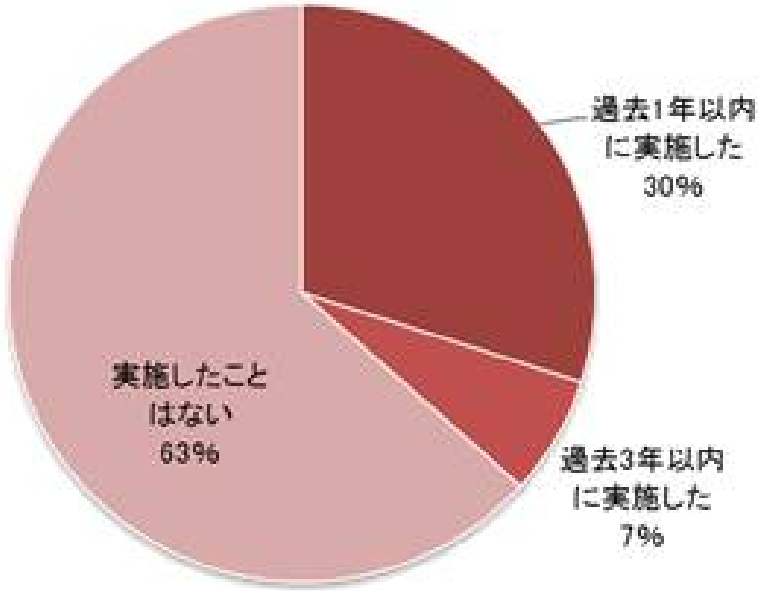
2. IT-BCP 訓練・演習の実施状況

2.1　民間企業の状況

IT-BCPの訓練：本番機の停止を伴うIT-BCPの訓練を実施していますか？
（回答企業数：30社）

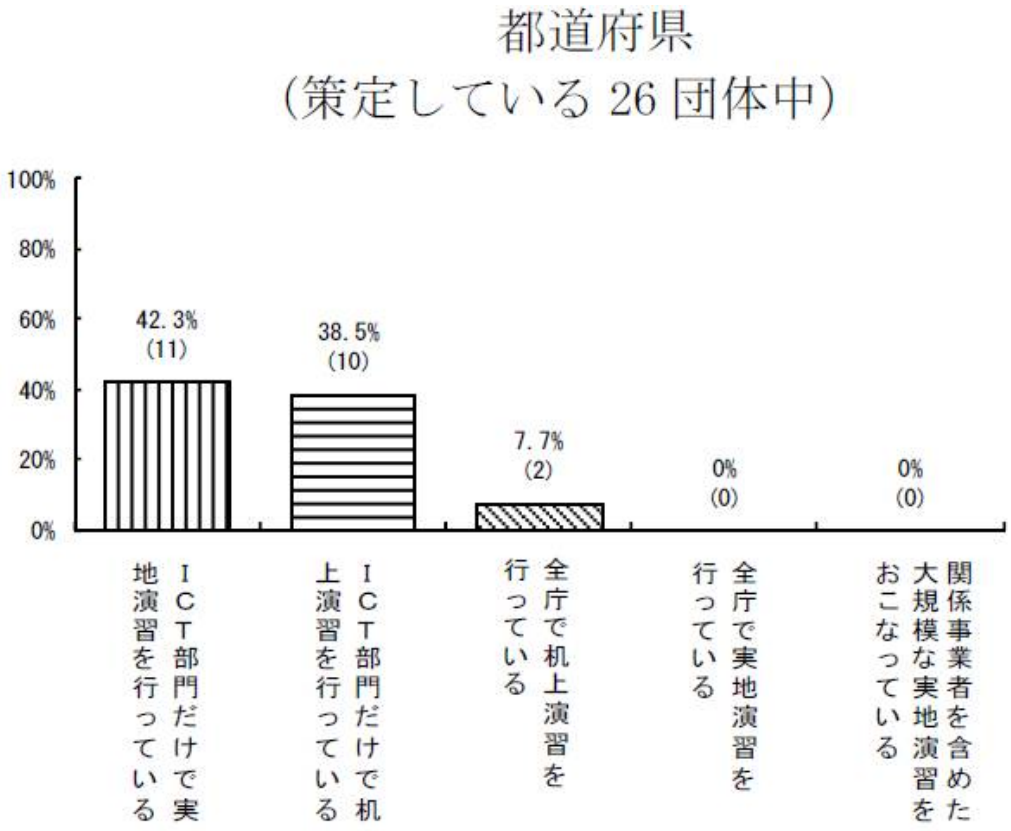


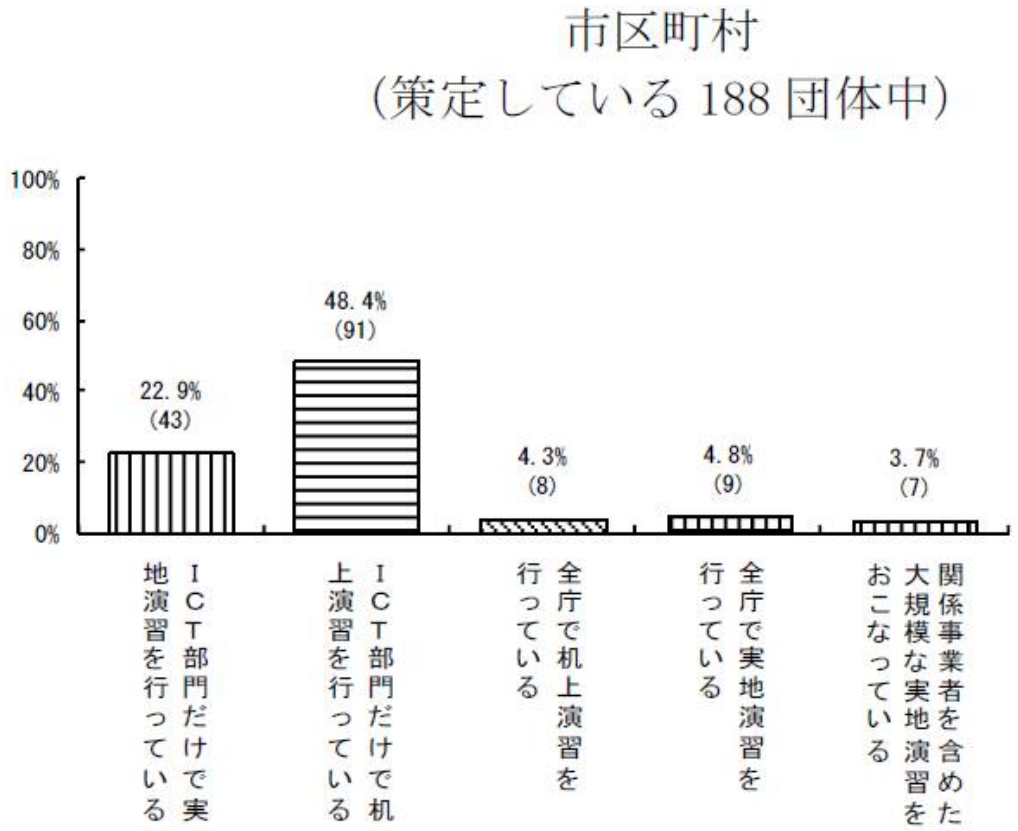
IT-BCPの訓練：ユーザー部門などを巻き込んでIT-BCPの訓練を実施していますか？
（回答企業数：30社）



出典：「IT-BCPサーベイ2013」プライスウォーターハウスクーパース株式会社 2013年

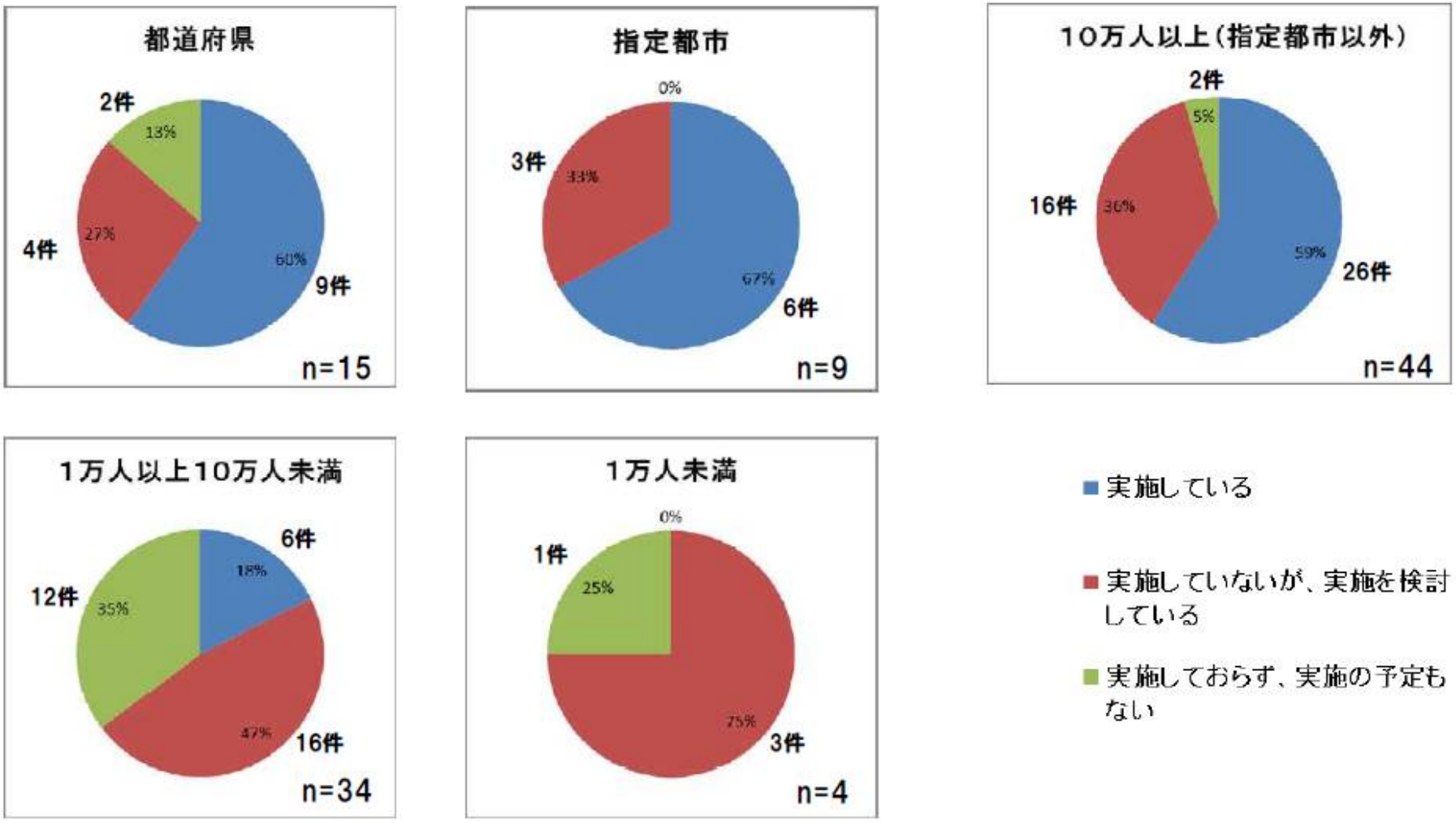
2.2 自治体の状況　(1 0f 2)





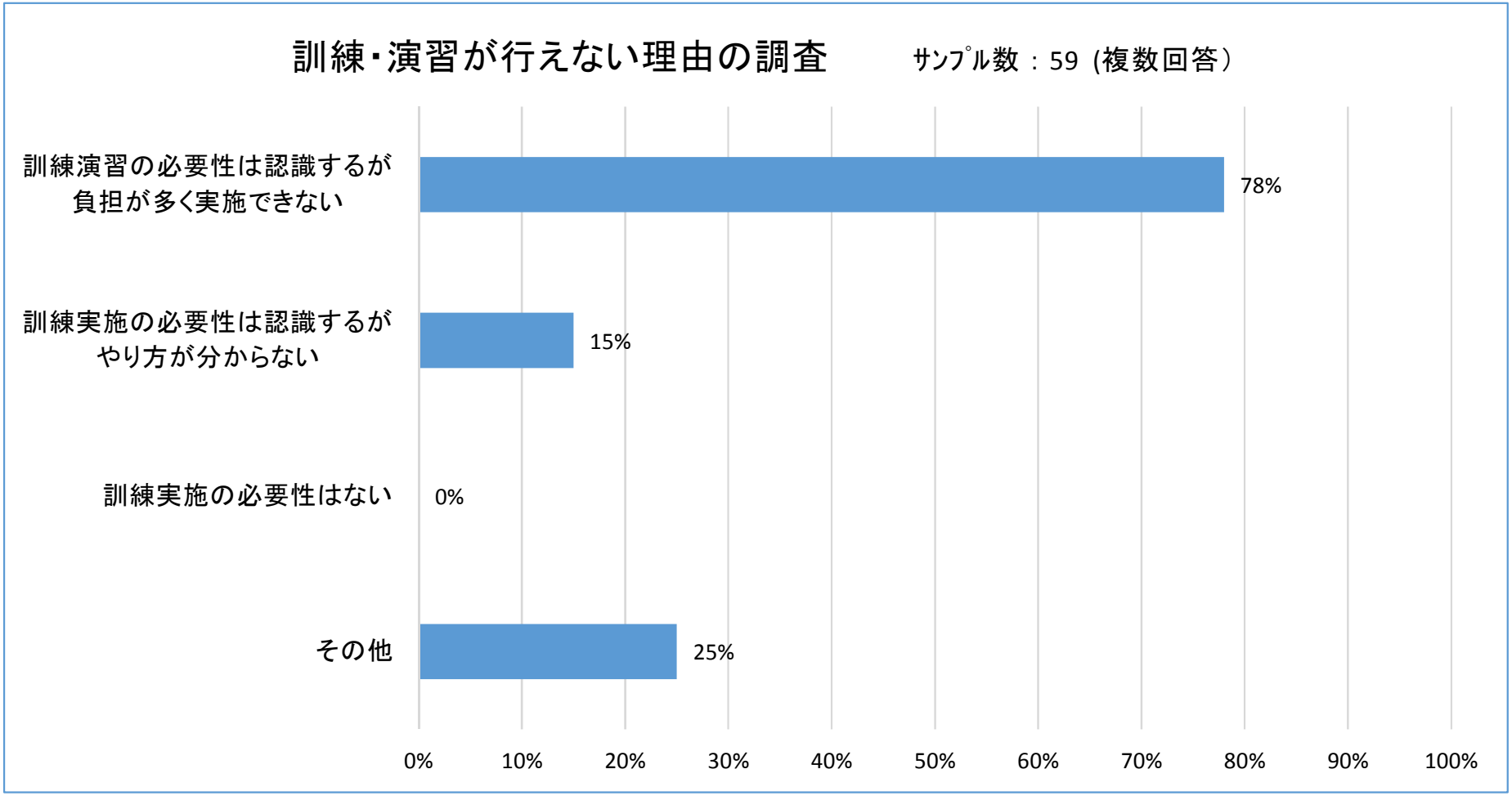
出典　：「地方自治情報管理概要 電子自治体の推進状況」 総務省（平成25年4月1日現在）26年3月公表

2.2 自治体の状況　(2 0f 2)



出典　：「災害発生時の業務継続及びICT の利活用等に関する調査にかかる補足調査」総務省 平成24年

2.3 BCP訓練未実施の理由



出典 ：「災害発生時の業務継続及びICT の利活用等に関する調査にかかる補足調査」総務省 平成24年

2.3 BCP訓練未実施の理由 （分析）

★「負担が大きい事」、「やり方が分からない」という理由が多い。

★「その他」と回答された組織から本番業務システムに対する影響を懸念して次のようなコメントが上げられている。

① 実機訓練の場合、本番運用への影響・調整や、訓練によるトラブルの発生のリスクがあるため

② 訓練中の操作により予想外のトラブルが発生し、通常業務に影響が出る懸念がある。

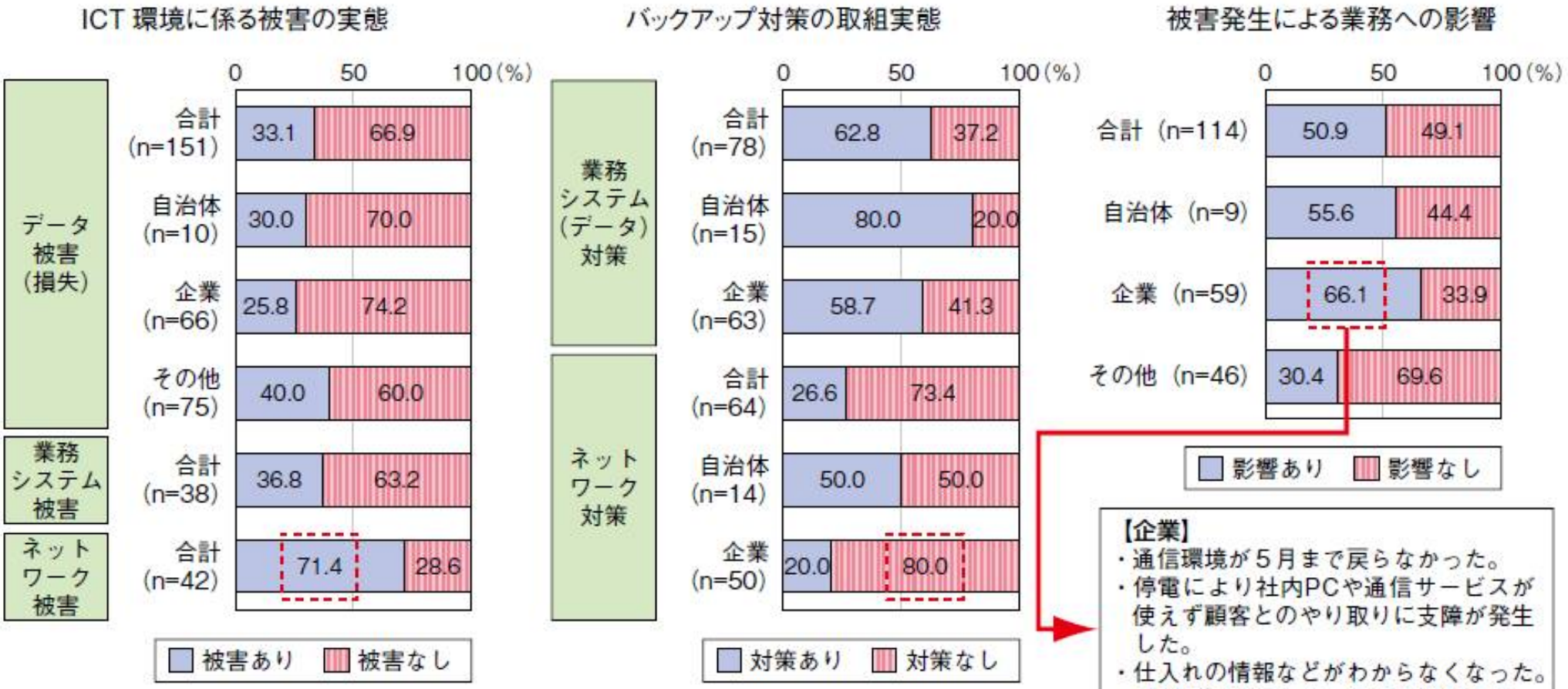
③ 情報機器はほぼすべての業務に関係しており、訓練の実施により停止する業務が発生し、市民サービスに影響するため困難である。

出典 ：「災害発生時の業務継続及びICT の利活用等に関する調査にかかる補足調査」総務省 平成24年

・・・＞「負担が少ない訓練・演習の方法」や「本番機に影響を与えない訓練・演習の方法」を周知できれば、訓練・演習を実施する組織が増えるのでは？

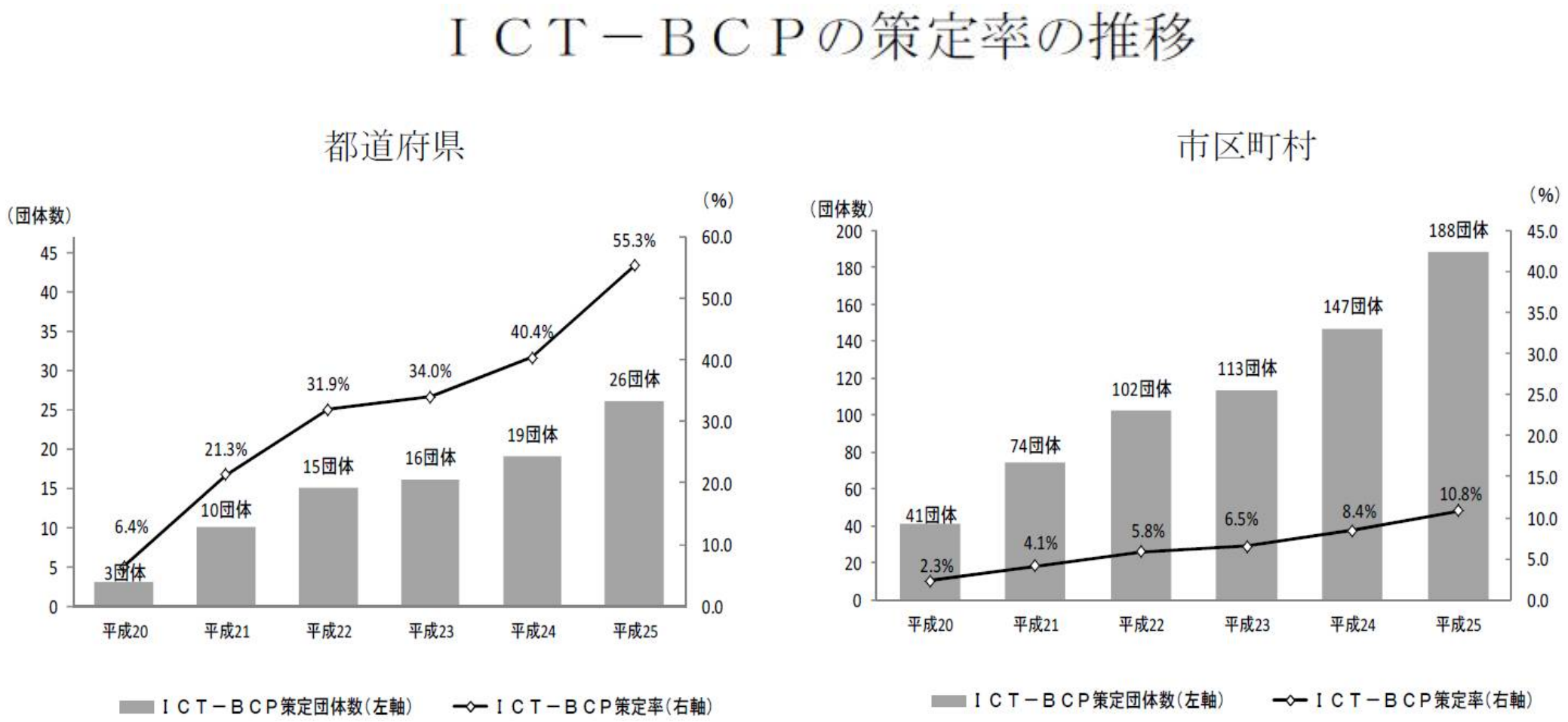
＜参考＞ IT-BCP の実効性検証

東日本大震災で情報システムへ被害 ～ 業務に影響



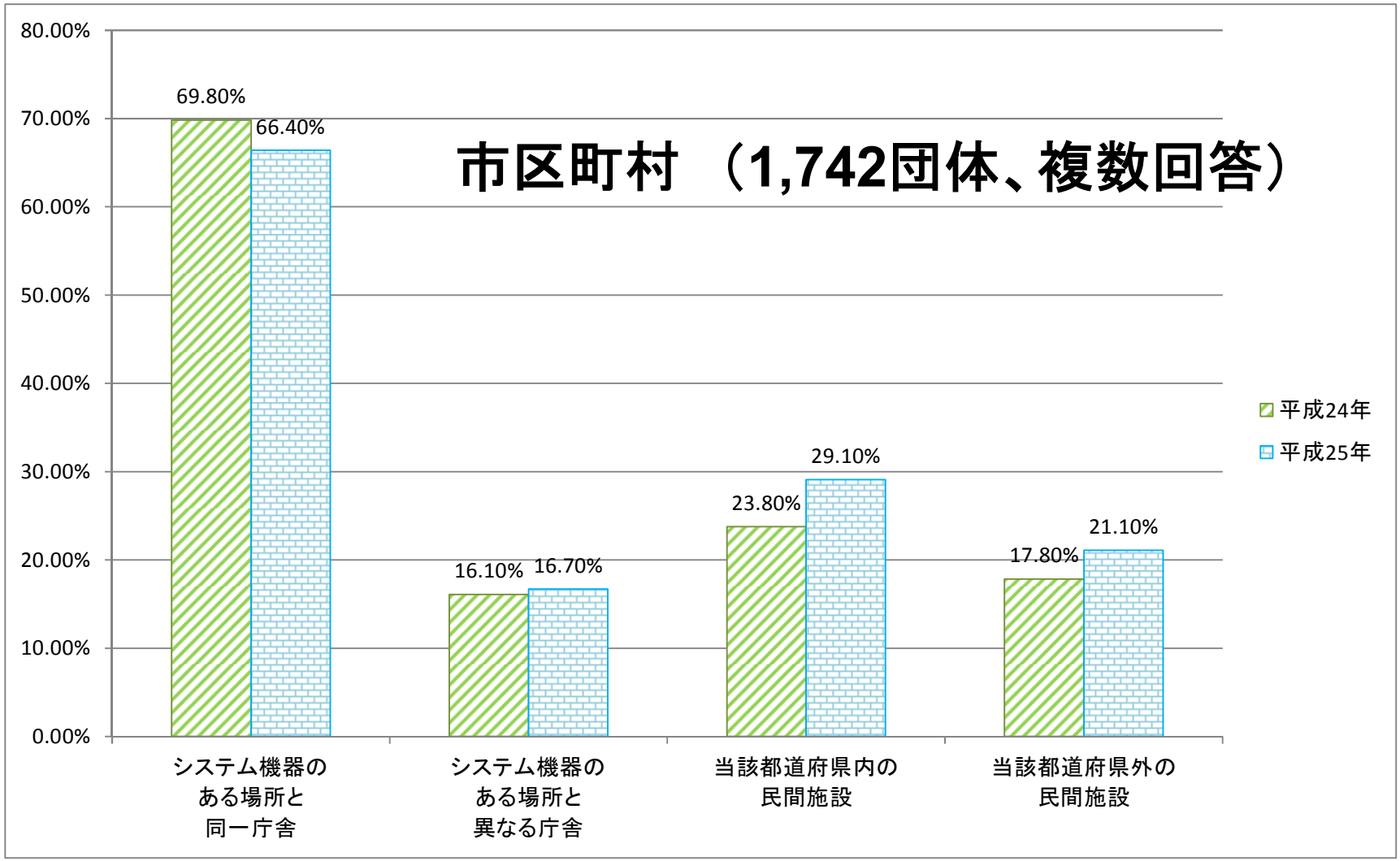
（出典）総務省「災害時における情報通信の在り方に関する調査」（平成 24 年）

＜参考＞ 情報システムに関する業務継続計画（BCP）の策定推移



出典 ：「地方自治情報管理概要 電子自治体の推進状況」 総務省（平成25年4月1日現在）26年3月公表

＜参考＞ 住民基本台帳ﾃﾞｰﾀのﾊﾞｯｸｱｯﾌﾟの保管場所



出典 ：「地方自治情報管理概要 地方公共団体における行政情報化の推進状況調査結果」 総務省 を元に加工

3. 実機テストで得られる気付きと改善

3．1　実機テストにより発生した主な事象

・手順書の不具合（メーカー提出、自社作成の両方）

コマンドのスペル間違い
手順書の操作順序間違い
手順書に抜け・漏れがあった
本番機とテスト機・予備機では差異がある

・作業員の経験不足によるミス

焦りによる、手順書の見間違い、見落とし
思い込みによる誤操作

・システムの不具合

起動できない、想定外の動作をする
本番機と予備機が完全に同一の設定になっている
本場機に適用した更新が予備機になされていない
メーカー間の認識違いで通信が出来なくなる

3．2　実機訓練の成果

・手順書の見直し
　　間違いや抜け漏れの修正
　　実運用に基づいた内容への変更
　　初期には考えられていなかった内容を追加

・作業員の経験の蓄積
　　2度目以降は操作への不安感がなくなり、ミスが減少
　　初期テストほど想定外の事象が起きやすい為、色々な経験ができる

・システムの不具合修正が完了
　　システム自体の問題が減少

4. 机上訓練で得られる気付きと改善

4. 1 机上訓練　DIGの紹介

有効な机上訓練のやり方として、
IT版のDIG を考案

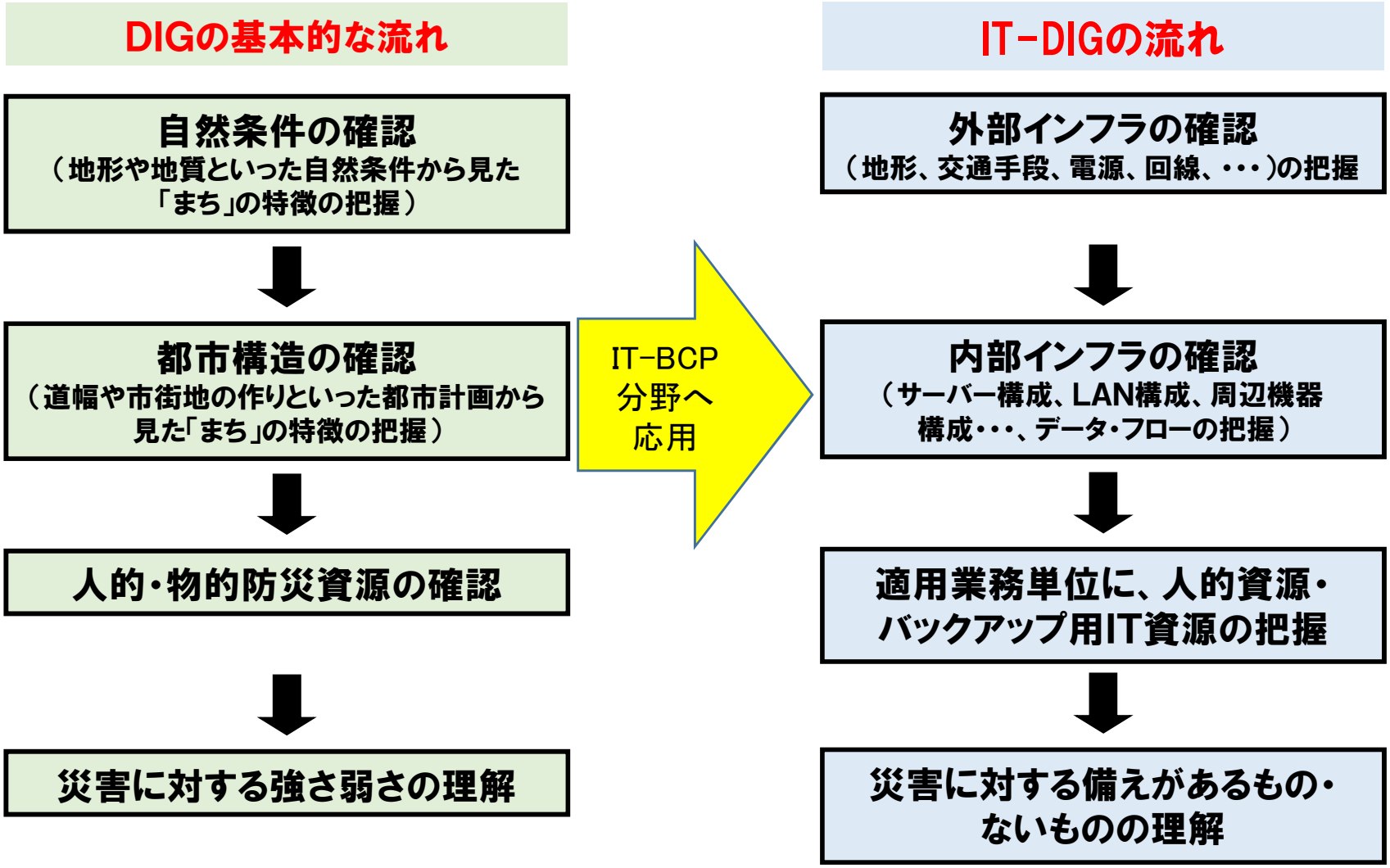
・DIGとは　　・・・　　災害 (Disaster)
想像力 (Imagination)
ゲーム (Game)
の頭文字を取って名付けられた、

1997年に当時三重県消防防災課に勤めていた平野昌氏他数氏の協力で開発されたものであり、一般市民が独力でも企画・運営できる簡易型の防災図上訓練ノウハウである。

＜参考＞　災害図上訓練 DIG の資料　「市区町村による風水害図上型防災訓練の実施支援マニュアル」
http://www.fdma.go.jp/neuter/topics/houdou/h23/2305/230525_1houdou/02_houdoushiryou.pdf

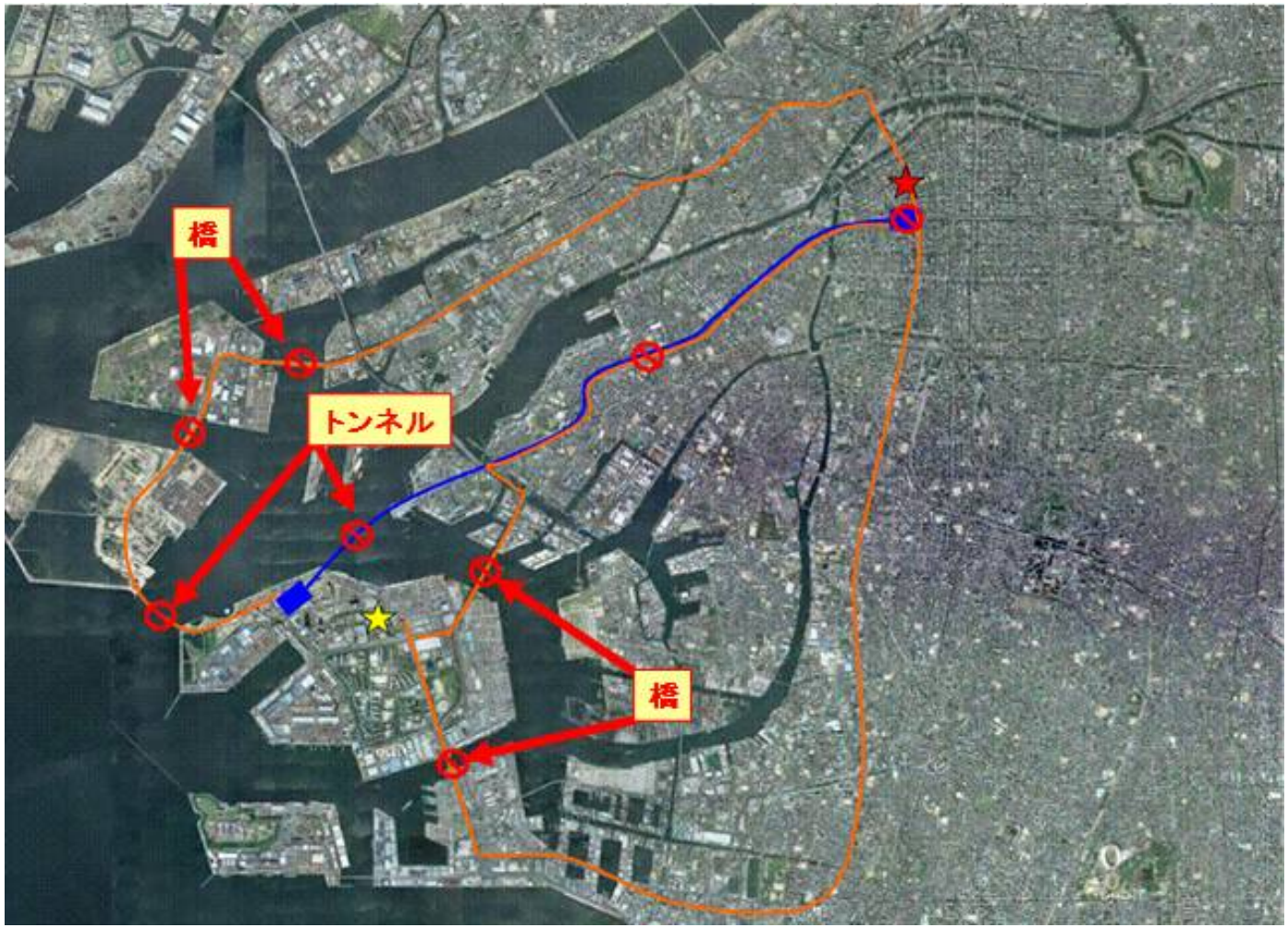
4．2　IT版 DIGの作成

◆DIGの応用方法

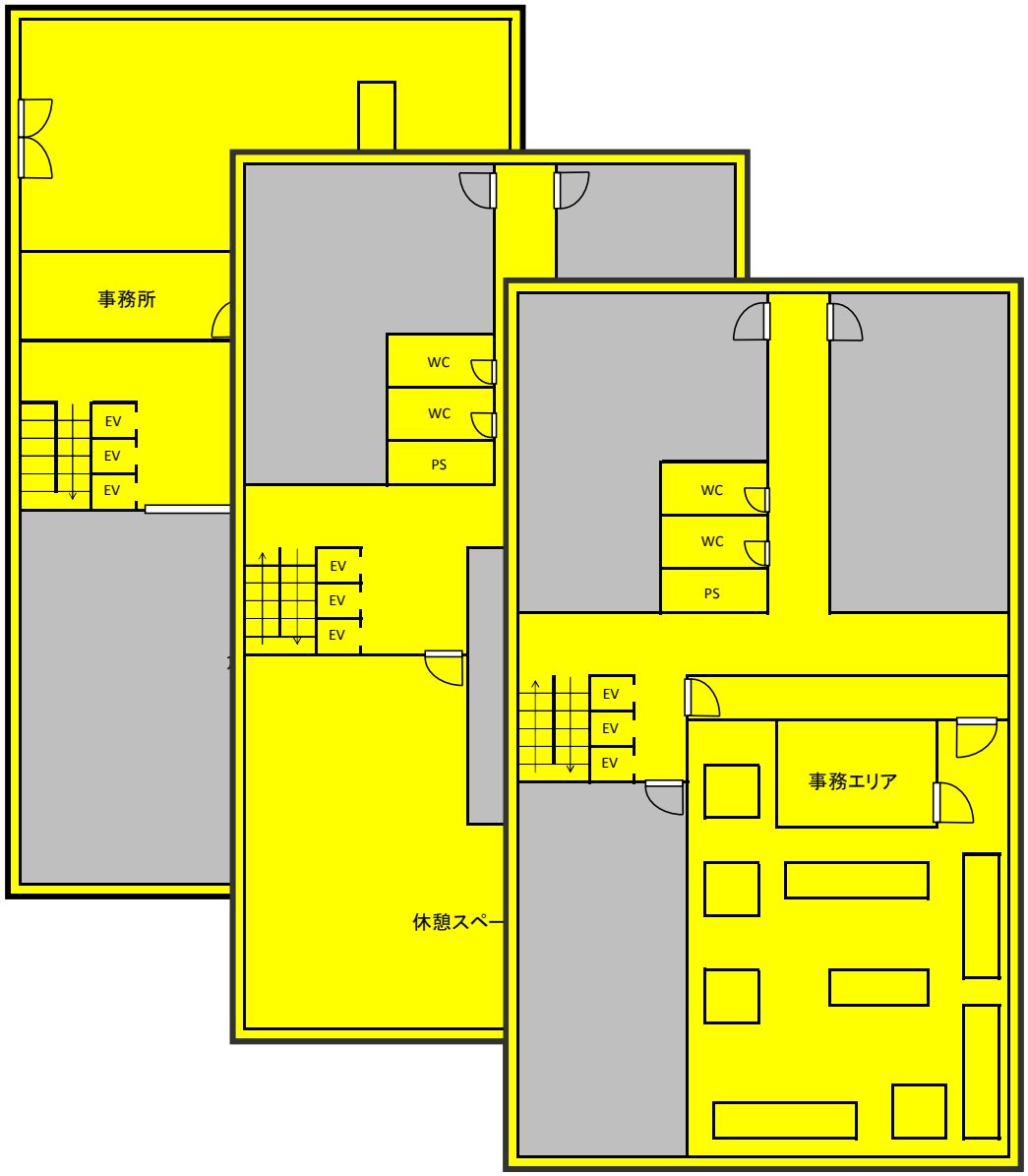


4. 3 ① IT版 DIGの実践 （外部インフラ）

＝リスクのある場所



4.3 ② IT版 DIGの実践（データセンター内_1）

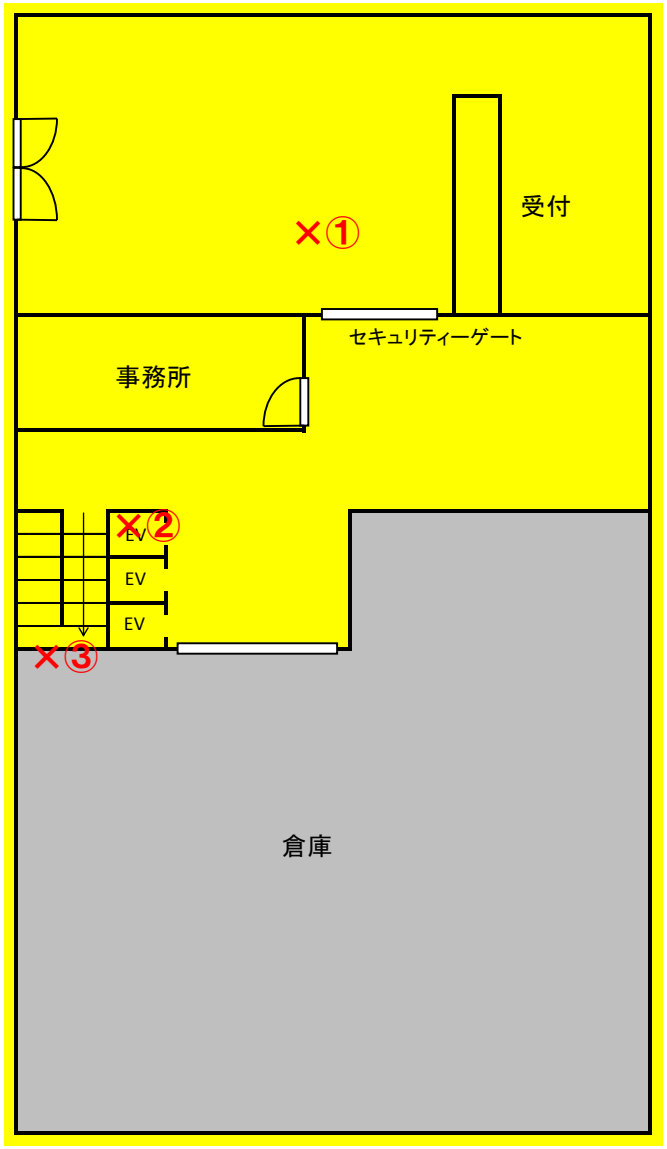


データセンターの概要

- 海抜は？
- サーバ室の海抜は？
- 非常用発電機はどこ？
- 自家発電は何時間駆動できる？
- NW回線はどこからの引き込み？

4.3 ② IT版 DIGの実践（データセンター内_2）

1F



①入館（セキュリティゲート）
被害の想定＞入館方法は？
対応策　　＞　・・・

②エレベータ
被害の想定＞緊急時にエレベータは使えるか？
対応策　　＞　・・・

③階段
被害の想定＞階段の広さは機材搬入か？
対応策　　＞　・・・

④消火装置
被害の想定＞消火装置の特性は？
対応策　　＞　・・・

4.3 ③ IT版 DIGの実践 人的資源

◆適用業務単位に、人的資源の把握

・通常時の人員配置から検討
①データーセンタで起こり得る障害を復旧するには何人必要か（検討）
②事務所側に復旧のための人員が必要か

・IT-DIGの結果
①サーバールーム内部
最小人員は？

②事務所
最小人員は？

4.3 ④ IT版 DIGの実践　バックアップ用 IT資源

◆適用業務単位に、バックアップ用IT資源の把握

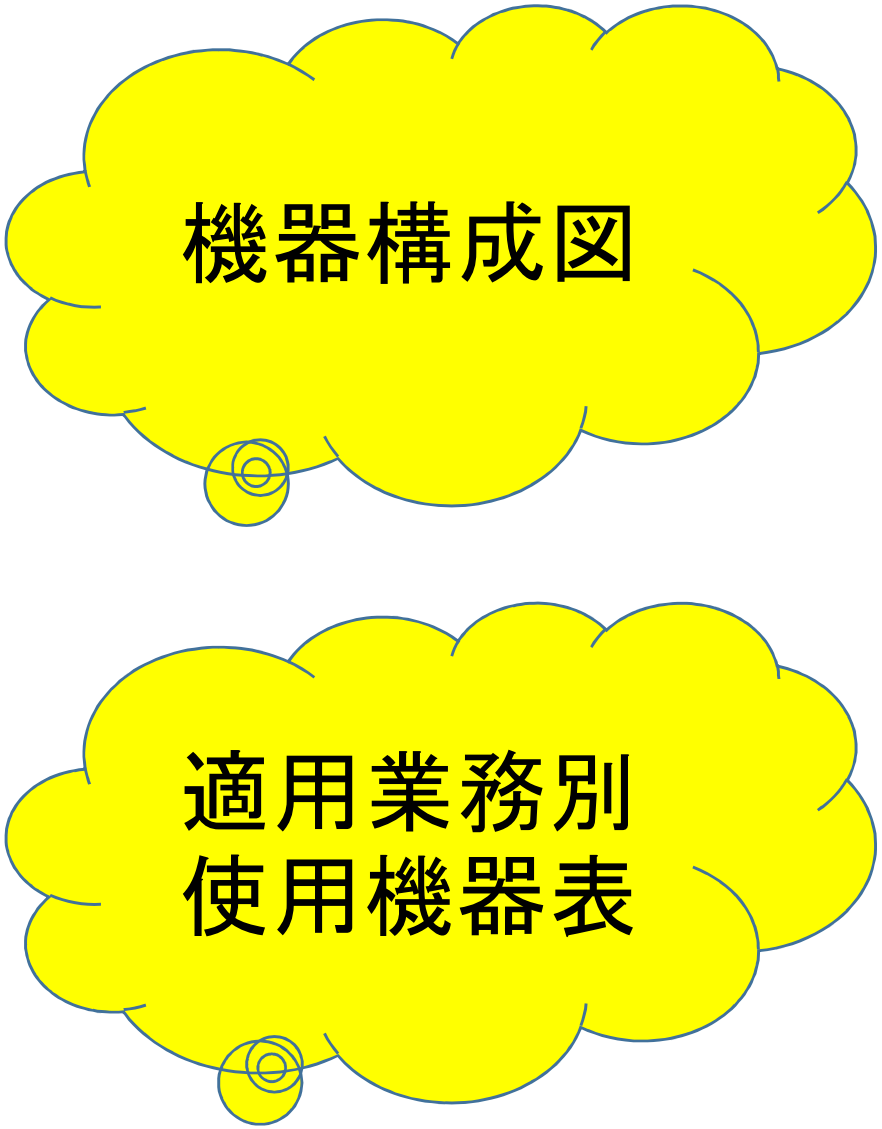
・データセンタ及び事務所内のバックアップ用IT資源の確認
①復旧に必要な機材はどのようなものがあるか
②機材の移送・搬入出は可能か

・IT版 DIGの結果
①既にバックアップがあるサーバ機器の他に、ネットワーク機器、
LANケーブル、電源ケーブル、電話線、テーブルタップ等
予備機器が用意されていないものにも障害の可能性があった。

②データセンタ内、事務所内は複数の搬入出経路があり、近隣階層に
あるため搬入出は可能だが、拠点間の移送は
交通上の問題でリスクが多く、現実的ではないと考えた。

→拠点内に準備がない機器が必要になった場合は、
復旧が予定通りに進まない可能性(リスク)がある。

＜参考＞ システム構成図から冗長度の考察



かなり以前から行われてる手法

＜構成要素の被害想定とその影響を検討する＞

① XXX に冗長度が無い
被害の想定⇒XXX の単一障害でシステムの
運用ができなくなる
対応策　⇒予備機を搬送して・・・

② YYY に冗長度が無い
被害の想定⇒障害時に・・・・運用が出来ない
対応策　⇒当該処理は緊急性が低い
ので障害復旧後に再開させる

システム自体は設計時に冗長性を或る程度意識して
構築されているため、大きな問題は出にくいが・・・
被害の想定が見えても設計段階から割り切っている場
合がある。（予算面等の理由）

4.3 ⑤ IT版 DIGの実践　備えの有無の確認

◆災害に対する備えがあるもの、ないものの理解と対策

・複数の対応策が考えられる場合、判断基準をできる限り
明確化しておく必要がある。 同時に「判断する人」
（指揮命令系統）も明確化しておく必要がある。
→例えば、「データセンターに連絡がつかず状況が不明な場合、
○時間経過した時点で・・・が止まっていたら、
プランAは諦め、プランBに移行」など

・意外に「外部環境」に不安要素が多い事が分かった。
→自社で復旧できない要素に関しては、代替案を事前に
用意しておくべき。

・手順書等の保管先に関しても災害時の被害を想定した上で
決定したほうが良い。
→緊急時の連絡網(取引先一覧やベンダーの連絡先など)も手順に
含められているべき。

4.5 IT版 DIGのまとめ （利点）

①外部インフラを含むシステム環境全体を可視化することで、詳しい知識がない人でも参加可能

→ 詳細な業務内容や機器構成を知らない他社メンバーでも、IT-DIGにより可視化された材料があった事で、高いレベルで議論ができ、新たな視点からの気付きにつながった。
また、見落としがちな「外部環境」に対する気付きも多くあった。

②手軽、簡単に実施できる

→実施に手間がかからないので、繰り返し実施しやすい。
既存の簡単な材料でも実施ができる。

③『正解』がないため、色々な意見が出やすい

→「間違い」はなく、全てが「気付き」になるので、参加者の心理的な敷居が低く、意見を出しやすい。

4.5 IT版 DIGのまとめ （注意点）

①確認できる内容に限界がある
　　復旧までの実測時間や、コマンドのスペルミスなど、
　　実機訓練でなければ確認できない内容もある。
　　→可能であれば、実機訓練も行うとなお良い。

② IT版 DIG不参加者への情報共有が難しい
　　実際にIT-DIGに参加した人間と、結果だけ伝えた人間では
　　理解に大きな差が出た。
　　→一部のスタッフで実施するのではなく、
　　BCPに関わる人間のなるべく多くが参加できるよう
　　繰り返し実施される事を推奨します。

4．5　IT版 DIGのまとめ　（実機訓練との比較）

実機訓練と机上訓練の比較

実機訓練を行う事による、リスクを伴う。
①本番機の稼働に悪影響を及ぼす危険性がある。
②テスト機でテストした手順が本番機で使えるとは限らない
③訓練の為にシステム停止をすることが難しい場合もある。

机上訓練ならば、実機訓練に伴うリスクを低減できる。
①本番系システムの稼働に影響を及ぼす危険がない。
　⇒　失敗が許される。
②実機を利用しないので、システム停止がない。
　⇒　本番系システムの運用時間の制約を受けない。

よって、先ずは机上訓練を行う事を推奨します。

4.6 訓練・演習への取り組み方の提案

訓練の必要性は認識されながら、「負担の大きさ」や「やり方が分からない」、「本番機への影響懸念」のために訓練が実施されていないという現状に対して・・・

① 比較的作業負担が軽く、本番機への影響が無い訓練として**IT版DIG**に取り組む

② 次に本番業務への影響が無い実機訓練として「**テスト機**」や「**予備機**」を使った訓練に取り組み、机上訓練の限界をカバーする

③ 最終的な確認として「**本番機**」を使った訓練に取り組み、テスト機による訓練の限界をカバーする

5. IT-BCPの実効性に関するシステム監査の視点

5.1 「システム管理基準」の中で当テーマに関係する主な事項

「趣旨」の出典：「システム管理基準の管理項目と統制目標の対応（例）【Excel形式】」 経済産業省
http://www.meti.go.jp/policy/netsecurity/downloadfiles/appendix_2.xls

イ. 組織体の長の承認

Ⅰ. 情報戦略
5. 事業継続計画
(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。
【システム管理基準の趣旨】:事業継続に関わる事象が発生した場合に全ての利害関係者が円滑に対応できるようにするため、利害関係者を含んだ組織体制で**実行性の高い事業継続計画**を立案し、組織体の長が承認する必要がある。

ロ. 従業員の教育訓練

(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。
【システム管理基準の趣旨】:事業継続に関わる脅威が発生しても、**迅速かつ確実に事業継続計画に定められた手続を実行**できるようにするため、事業継続計画には従業員の**教育訓練**の方針を明確にする必要がある。

ハ. 関係各部に周知徹底

(4) 事業継続計画は、関係各部に周知徹底すること。
【システム管理基準の趣旨】:**事業継続計画の実行性を高める**ため、事業継続計画を関係者に周知徹底する必要がある。

ニ. 見直しと更新

(5)事業継続計画は、必要に応じて見直すこと。
【システム管理基準の趣旨】:**事業継続計画の有効性を維持する**ため、必要に応じて見直し及び更新を行う必要がある。

5.2 システム監査の際に確認すべき事項

イ. 組織体の長の承認

組織体の長が承認を与えた記録の確認
組織体の長が次のリスクを正しく認識した事を確認する
- 「訓練をするリスク・しないリスク」
- 本番機を使うリスク・使わないリスク
- テスト機を使うリスク・使わないリスク
- 机上訓練の限界

ロ. 従業員の教育訓練

- 訓練参加者リストの確認
- 訓練で得た気づきや課題点を整理した文書の確認

ハ. 関係各部に周知徹底

- 関係部署の一覧リスト
- 関係部署に周知した記録の確認

ニ. 見直しと更新

- IT-BCP資料類が見直し・更新されている事の確認
- 関係部署へ最新版が配布されている事の確認

6. IT-BCP 想定外への備えは可能か？

＜問い＞　一応の ITｻｰﾋﾞｽ継続計画はあるが
想定外の事態への備えは可能か？

① 想定とは？

② 想定外の事態にも対応できるような準備は可能か？

③ IT部門としてどのような対処なら可能か？

東日本大震災の後、「それは 想定外」という話が・・・

過去問を全てマスターしたら司法試験に合格できるか？

「想定」とは何か？

「『想定外』を想定せよ」 畑村洋太郎著　NHK出版

物事を検討する「範囲」として
　　・・・　仮りに設定した 「制約条件」

＊費用（予算）の制約
＊検討時間・構築時間の制約
＊作業工数の制約

・・・「想定外」 は起こりえないのではなく、
確率は低いながら起こる可能性がある

【参考】 釜石の奇跡

（１） 釜石市は東日本大震災で甚大な被害を受けた

（２） しかし、小中学生の殆どは無事であった

市内１４校の約３０００人の小中学生のうち

９９．８％ の生徒達が助かった

（３） 奇跡を起こしたのは日頃の備え

・どんな備え？

【参考】 事前の準備有無と対応の可否

		事前の準備	
		ある	ない
対応	できる		?
	できない	?	

6.1　訓練の段階的高度化

◇ステップ１　：手順書の内容に従って、作業が正しく完了できることを確認する

◇ステップ２　：予め設定された手順の途中で条件が変更されても、正しく作業を完了できるかどうかを確認する

テストの種類	実施内容	メリット	デメリット
ロールプレイング	・テスト実施の途中で状況を追加付与し、参加者の状況判断や意思決定の可否、連絡体制などを検証する。	計画を実行する判断者の訓練になり、判断資料の手当てなどが確認できる	想定状況を多数設定するため、事前準備の負荷は大きい。参加者の十分な知識も必要となる。必要要員は多い。

6.2 訓練の段階的高度化 ステップ 1

◇ステップ1 ：手順書の内容に従って、
作業が正しく完了できることを確認

〔訓練の目的・位置づけ〕
「事前の準備はあったが対応できなかった」 を未然に発見する。
テストを実施する事で、手順書の抜け漏れやシステムの不具合などを
発見でき、修正する事ができるようになる。
作業員が手順書の内容を正しく理解・実行できるかどうかも
同時に確認できる。

6.3　訓練の段階的高度化　ステップ 2

◇ステップ2 ： 予め設定された手順の途中で条件が変更されても、
正しく作業を完了できるかどうかを確認

〔訓練の目的・ 位置づけ〕

「事前の準備が無い」 という事態でも、「対応できる」力を養います。
人為的に想定外を作り出す事で、指揮官の判断力や作業員の
判断力・応用力を向上させる。
また、その結果を受けての事前準備の見直しなどにも繋げる事が
できる。

〔条件変更方法の例〕

グリーンカード（※1）・・・ 一部の「仕掛け人」が想定外を発生させる
ランダムトラブル&シナリオ発生カード　・・・訓練シナリオをランダムに設定

※1アメリカ航空宇宙局（NASA）で実施している、宇宙飛行士の訓練手法。

ご清聴ありがとうございました