ICT部門のBCP

止まらない？システムの実現方法

～3.11に学ぶ、ICT現場での現実的な事業継続の対策とは～

情報システム監査株式会社　　木村　修二

私の問題意識

自治体のIT－BCPの策定支援に携わってきた。
公共と民間の差を強く意識するようになった。
ここから、IT－BCPそのものを見直すこととなった。

自治体BCPについての3つの視点

1. 期間によってテーマが異なる
   初動期間（72時間）＋1週間
   復旧期間
   復興期間
2. 公共と民間ではテーマが異なる
   自治体のBCPは、地域の復旧・人命救助が目的。
   被災によって新たに発生する業務に全力を投入する。
   だから「業務継続計画」「業務縮退計画」である。
   民間とは組織の存立意義・目的が異なる。
3. 被災を少なくするために
   BCPの視点から身近な日常業務を見直す
4. 復旧を容易にするために
   BCPの視点から情報システムを見直す
   BCPの視点から情報セキュリティを見直す

災害対策基本法

防災基本計画

地域防災計画

地域の復旧

実現するために

地域が被災することを想定して、地域の復旧のために、
地域のみんなが防災計画・BCPをつくりましょう・・・

自治体の自組織内部

自組織を維持して地域の復旧に全力投入

自治体のBCP

地域内の他の組織

町内会・自治会・・・　家庭・個人

各種団体

企業

災害対策基本法での
企業の位置づけから
企業のBCPを考える

企業のBCP

自助、公助、共助、そして民助！

災害に強い電子自治体に関する研究会（中間報告）（案）
－ICT 部門の業務継続計画（ICT-BCP）ガイドラインの改訂の方向性について －

１．東日本大震災の教訓と現状認識

発災直後における**避難者の名簿作成**に加え、**名簿と住民情報の突合・確認**に困難を極めたほか、安否情報等の提供にも支障が生じた。さらには、住民情報システム等の停止は、各種証明書を利用して日常生活を取り戻そうとする住民のニーズに迅速に応じることを困難にした。このことが、被災者支援のスピードを鈍化させたとの指摘もある。

２．ガイドラインの改訂の方向性

当面、地方公共団体が最小限定めておくべき事項を、現行のガイドラインから切り出して明確化する。具体的には、**発災後概ね72時間**を念頭に置いた初動時対応にフォーカスして「**初動を可能とするためのアクション（「事前対策」を含む）**」をシンプルに切り出し、具体化の事例をあわせて提示する。

パラメタを整理してみよう

被害想定結果

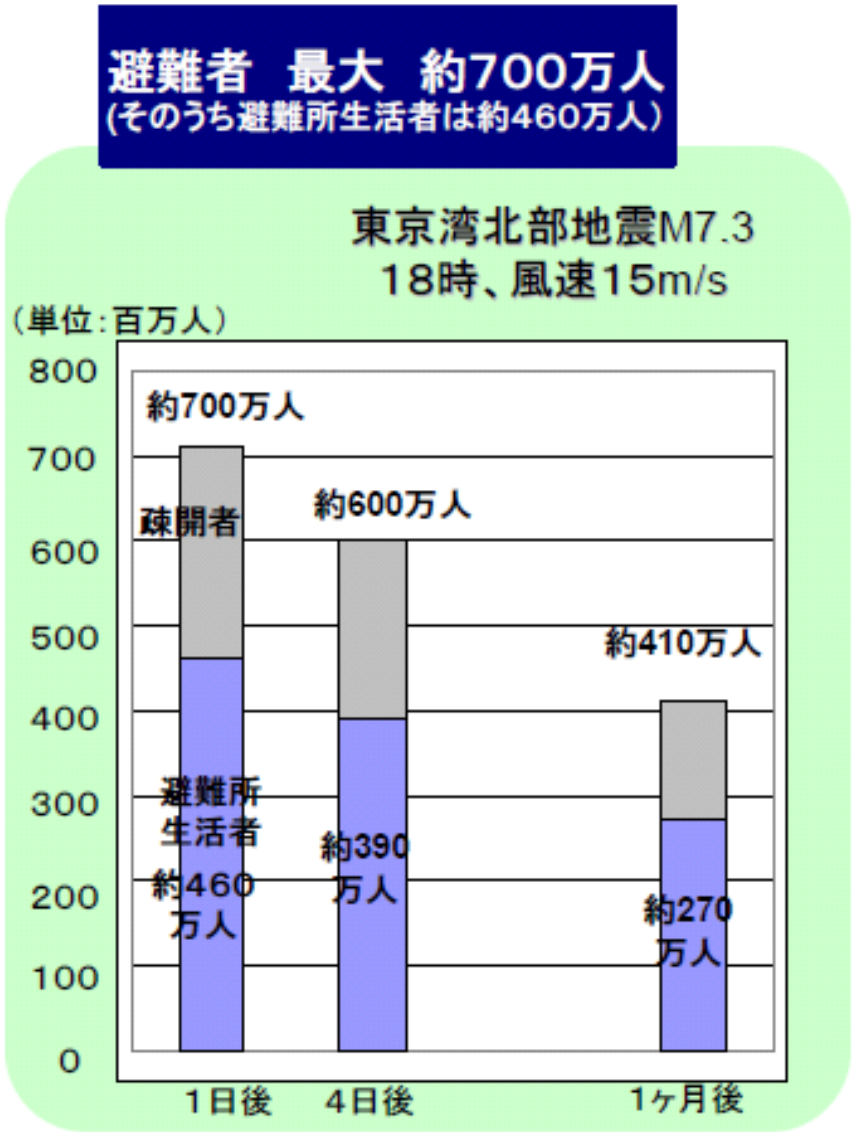
1－131

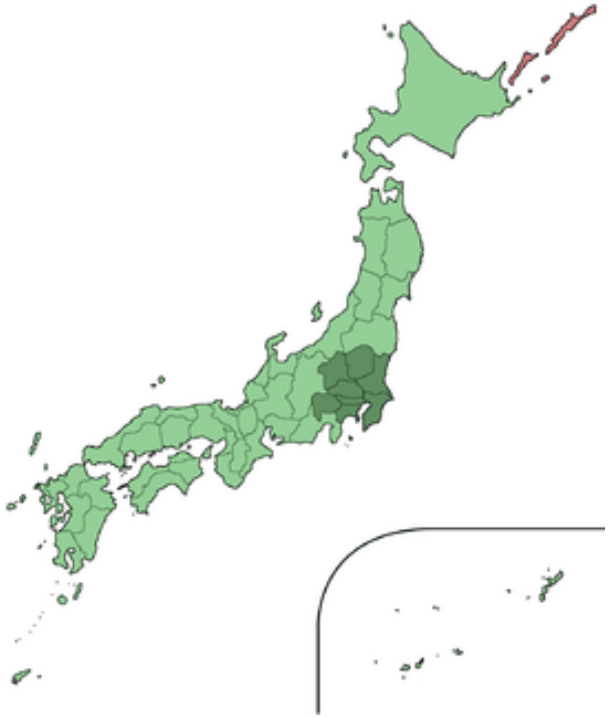
図表　既往地震災害時のライフライン復旧日数

項目	阪神・淡路大震災	東日本大震災	Bcpでの被害想定
電気	・停電約 260 万戸 ・発災 6 日後倒壊家屋等を除き復旧完了	【東北電力管内】 ・停電約 466 万戸 (3/11) ・発災後 3 日で約 80%の停電を解消 ・発災後 8 日で約 94%の停電を解消	3日間停電
固定電話	・交換機系:約 28 万 5 千回線不通 1 日後復旧完了 ・加入者系:約 19 万 3 千回線不通 14 日後復旧完了	・不通約 100 万回線 (3/13) ・発災後約 1 週間で約 80%の不通を解消 (4/20 約 20 万回線) ・発災後約 2 週間で約 90%の不通を解消 (4/26 約 10 万回線)	2週間不通
都市ガス	・供給停止戸数約 84 万 5 千戸 ・発災 85 日後倒壊家屋等を除き復旧完了	・供給停止約 46 万戸 ・発災後約 1 カ月で約 80%の供給停止を解消 (4/15 約 10 万戸) ・発災後約 2 カ月で約 90%の供給停止を解消 (5/4 約 6 万戸)	1か月停止
上水道	・断水約 127 万戸 ・発災 42 日後に仮復旧完了 ・発災 91 日後に全戸通水完了	・断水約 160 万戸 (3/17) ・断水約 30 万戸 (3/31) ・断水約 10 万戸 (4/20)	2週間停止
下水道	・被災管きょ総延長約 180km (兵庫県) ・発災 42 日後に仮復旧完了 ・発災 94 日後に全戸通水完了	・被害管路延長約 960km ・震災当初稼働停止処理施設 48 箇所のうち、津波等で約 3 カ月後も 18 箇所が停止 (6/6 現在)	1か月停止

物流は？(道路・橋梁・鉄道)

要員確保のパラメタ
重要な人的被害の数値予測





東京都市圏では定義にもよるが約3,400 - 3,700万人である。

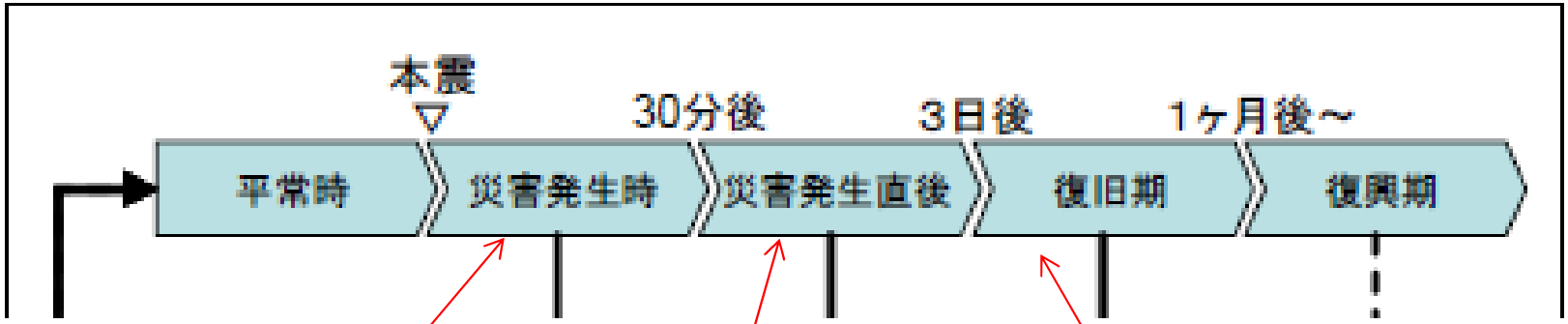
700万人÷3700万人＝19%

たとえば従業員出勤率
当日・・・・緊急対応要員のみ
2日目・・・30%
7日目・・・90%

http://activity.jpc-net.jp/detail/isd/activity001044/attached.pdf

「東日本大震災に学ぶ 今後のICT活用のあり方」に関する調査報告

2011 年8 月4 日　情報化推進国民会議



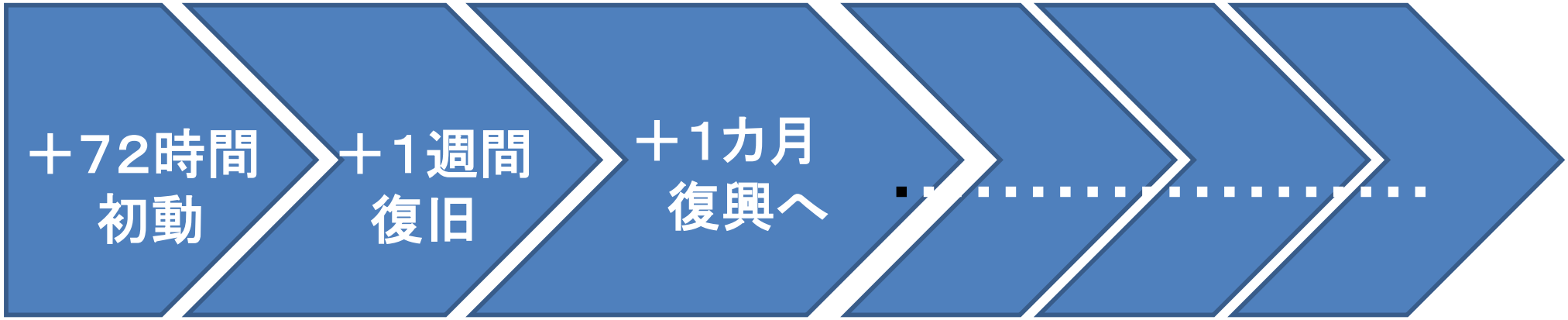
本震発生から概ね30 分後まで。
（津波の第1 波が到来するまで）

災害対策本部を立ち上げ避難者の安全確保に向けた行動を起こすと共に、逃げ遅れた人々等の救助活動が重点となる。

本震の概ね3日後から1ヶ月後まで（被災状況によっては数ヶ月後まで）。
避難・救助から生活の回復へと重点が移り、被災者の安全確保の継続と、健康維持、的確な医療の供給などがポイントになるものと想定した。

時期によってテーマが異なる･できることが異なる

避難･救助 ⟶ 生活の回復



電源　３日間

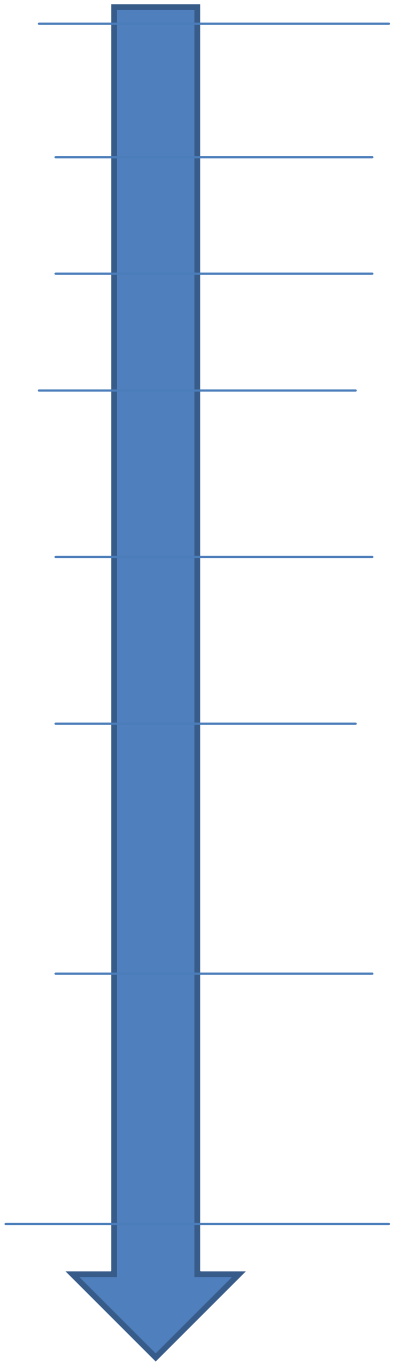
応援　１週間

通信　　２週間

上水道　２週間

都市ガス　１か月

下水道　　１か月



災害発生

災害対策本部立ち上げ

＋2時間

HPで第1報

避難所開設

＋4時間

住民の安否確認

＋6時間

追加食糧供給

＋12時間

＋24時間

ここで行う業務はすべて緊急対策業務
通常業務はすべてストップして、
人命救助へ全力投入！

＋48時間

だから、業務継続計画ではなく、
「業務縮小計画」

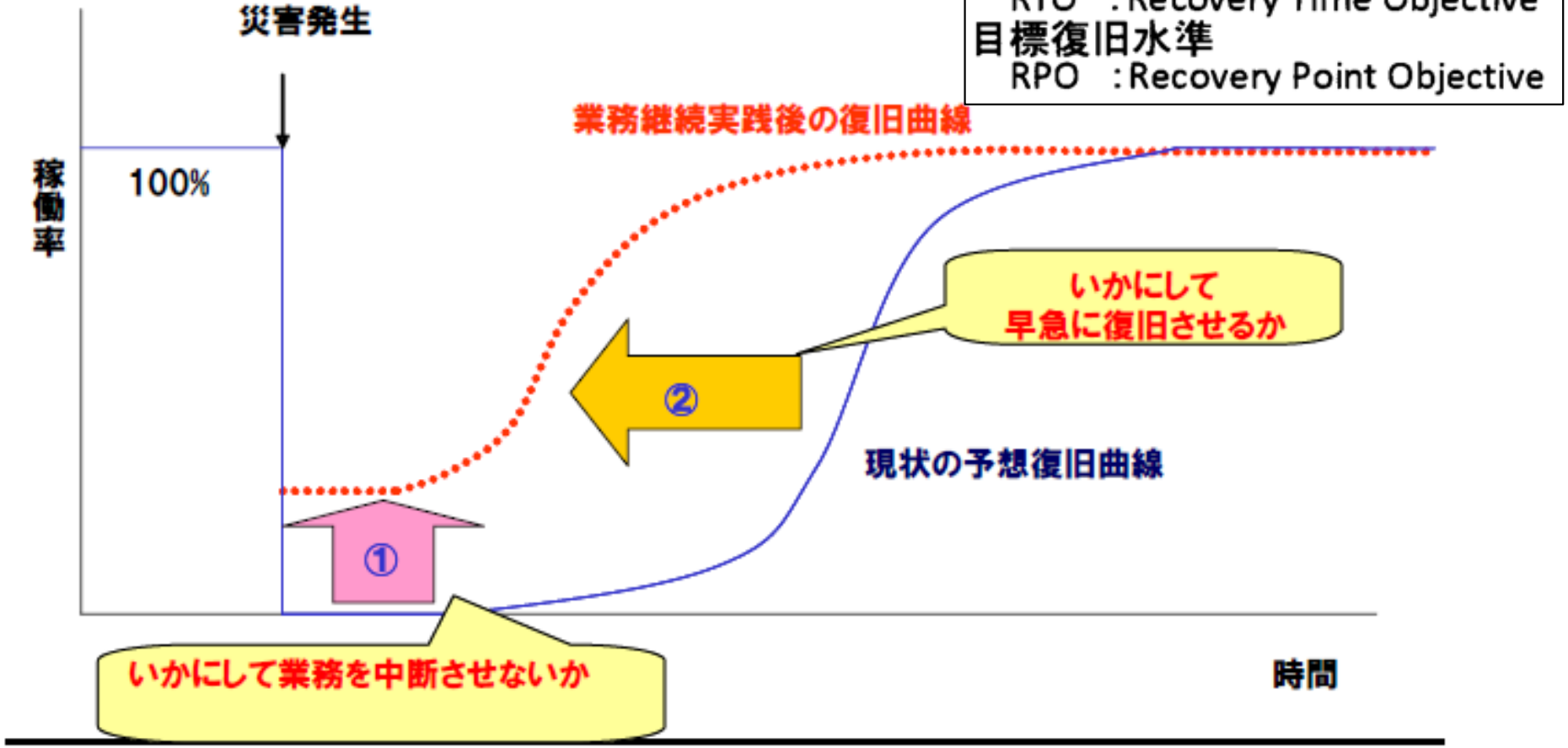
＋72時間

業務継続計画とは

「業務継続計画」とは、災害・事故で被害を受けても、重要業務をなるべく中断させず、中断してもできるだけ早急に（あるいは、許容される中断時間内に）復旧させる「業務継続」を戦略的に実現するための計画である。

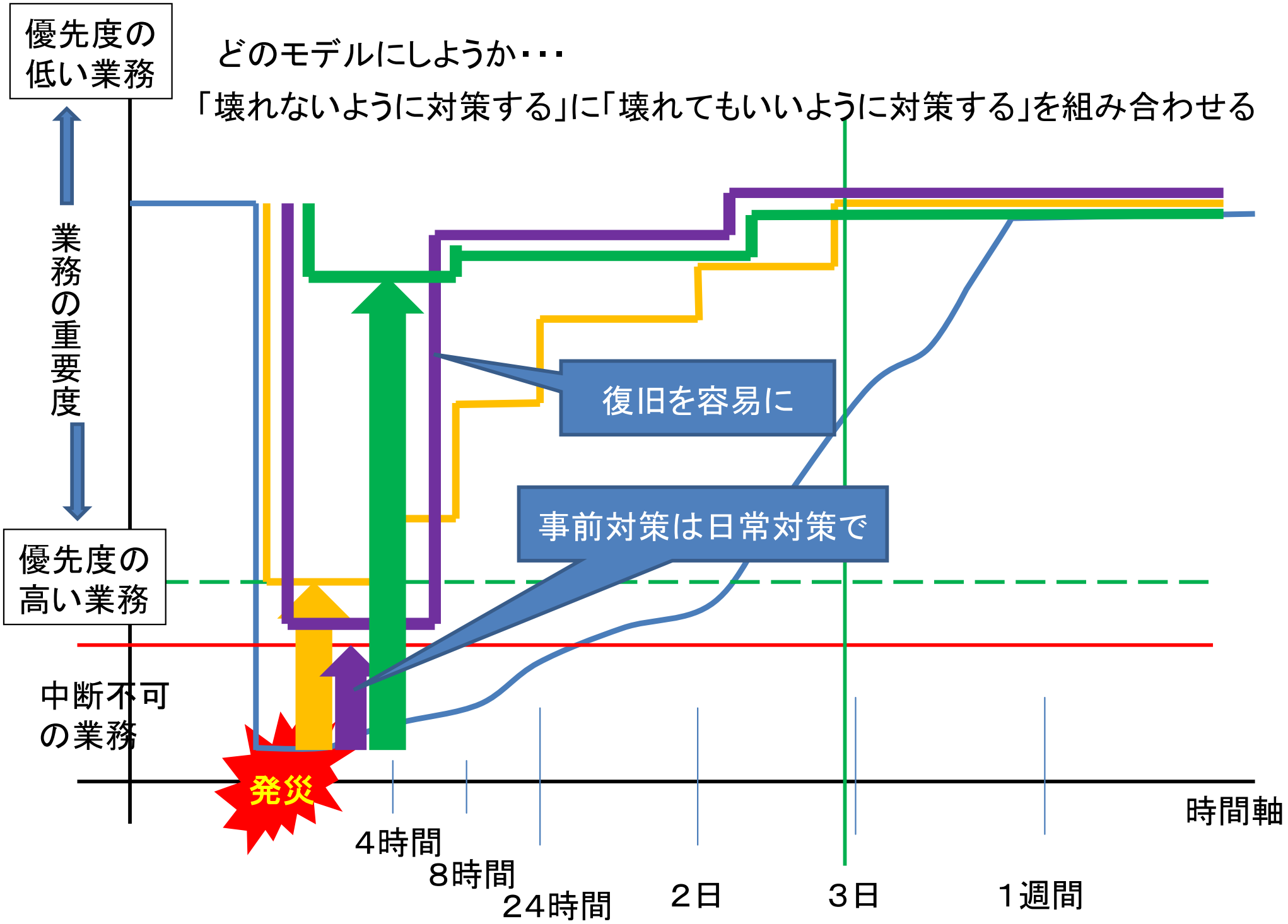
最大停止許容時間
MTPD：Maximum Tolerable Period of Disruption
目標復旧時間
RTO　：Recovery Time Objective
目標復旧水準
RPO　：Recovery Point Objective

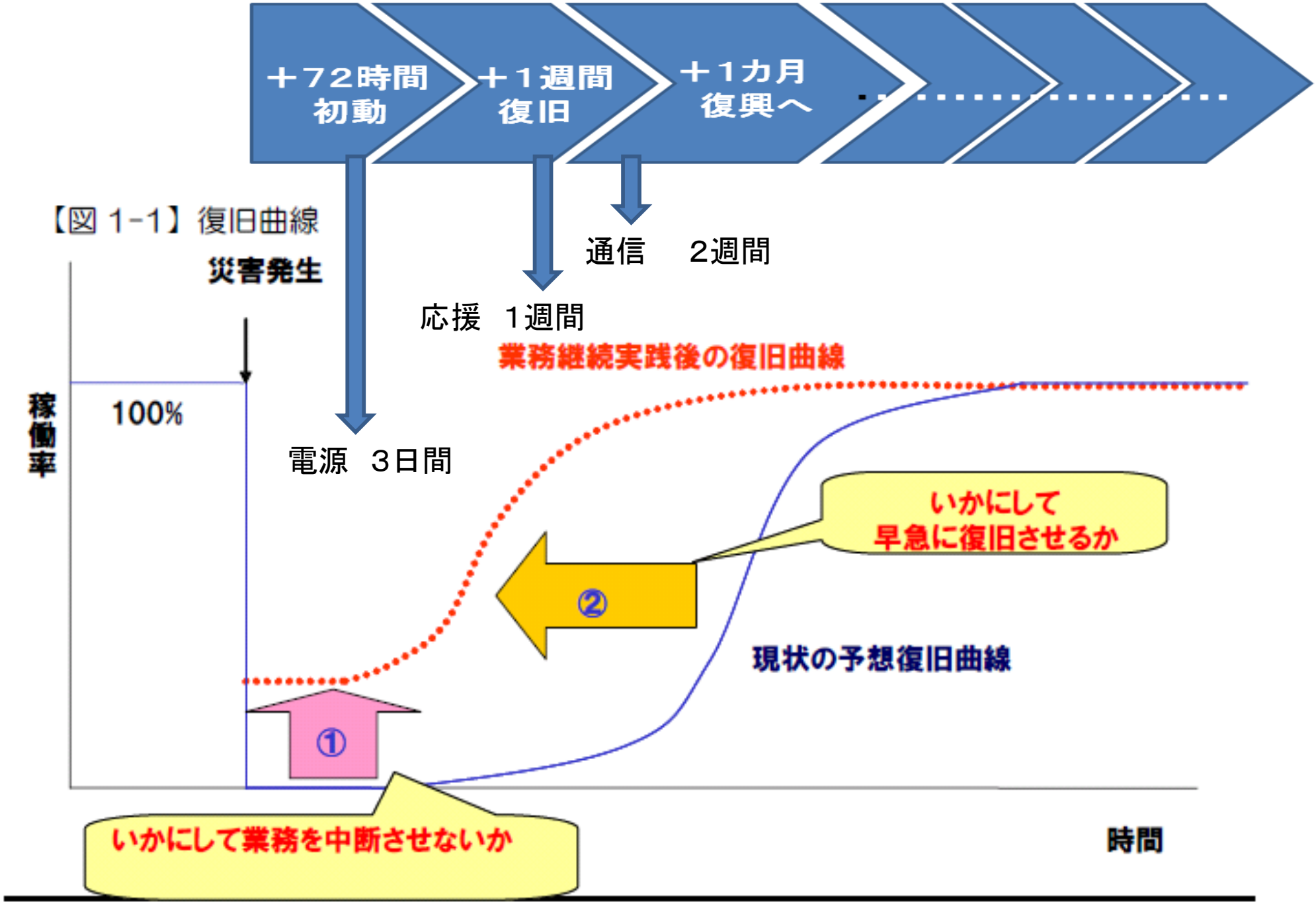
【図 1-1】復旧曲線

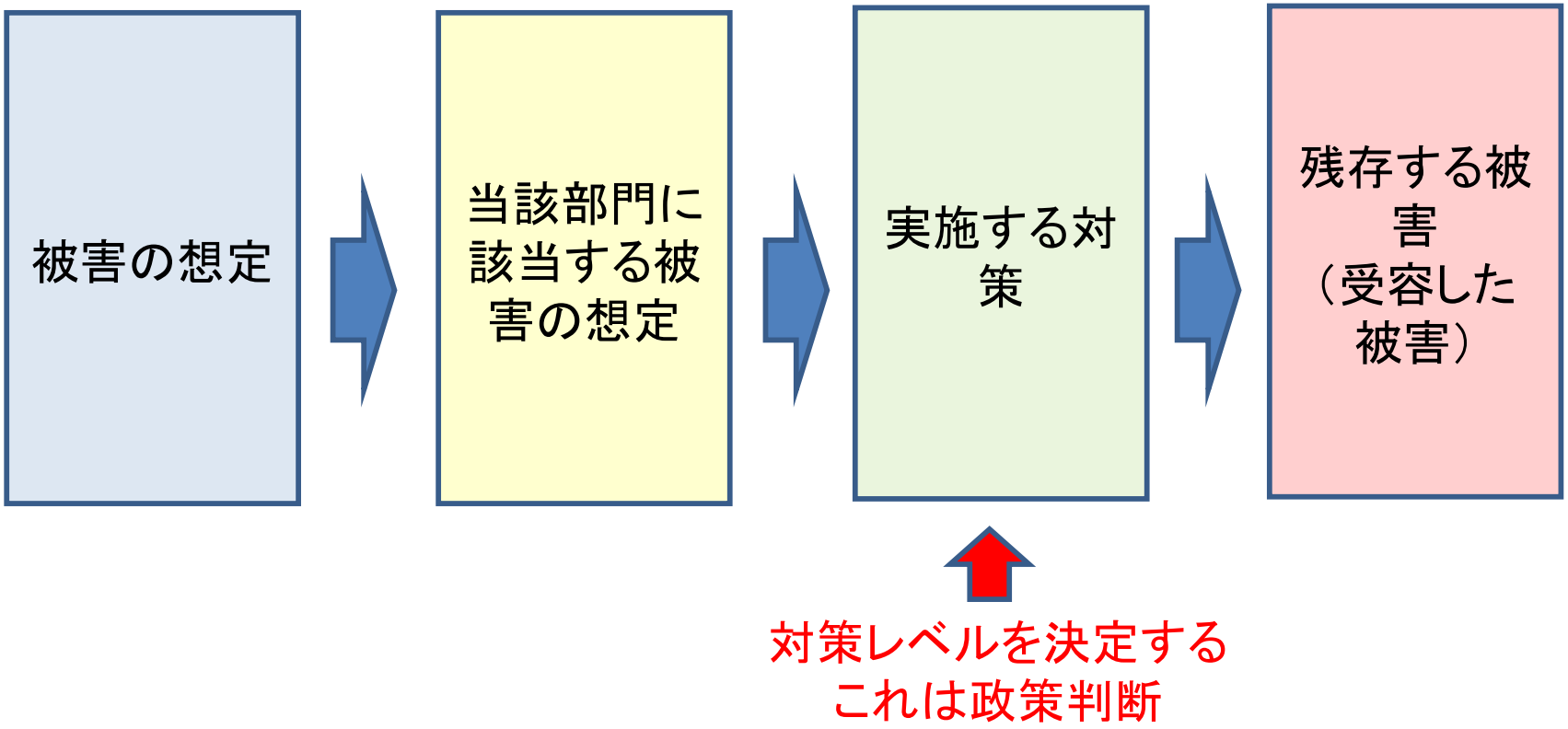


どのモデルにしようか・・・

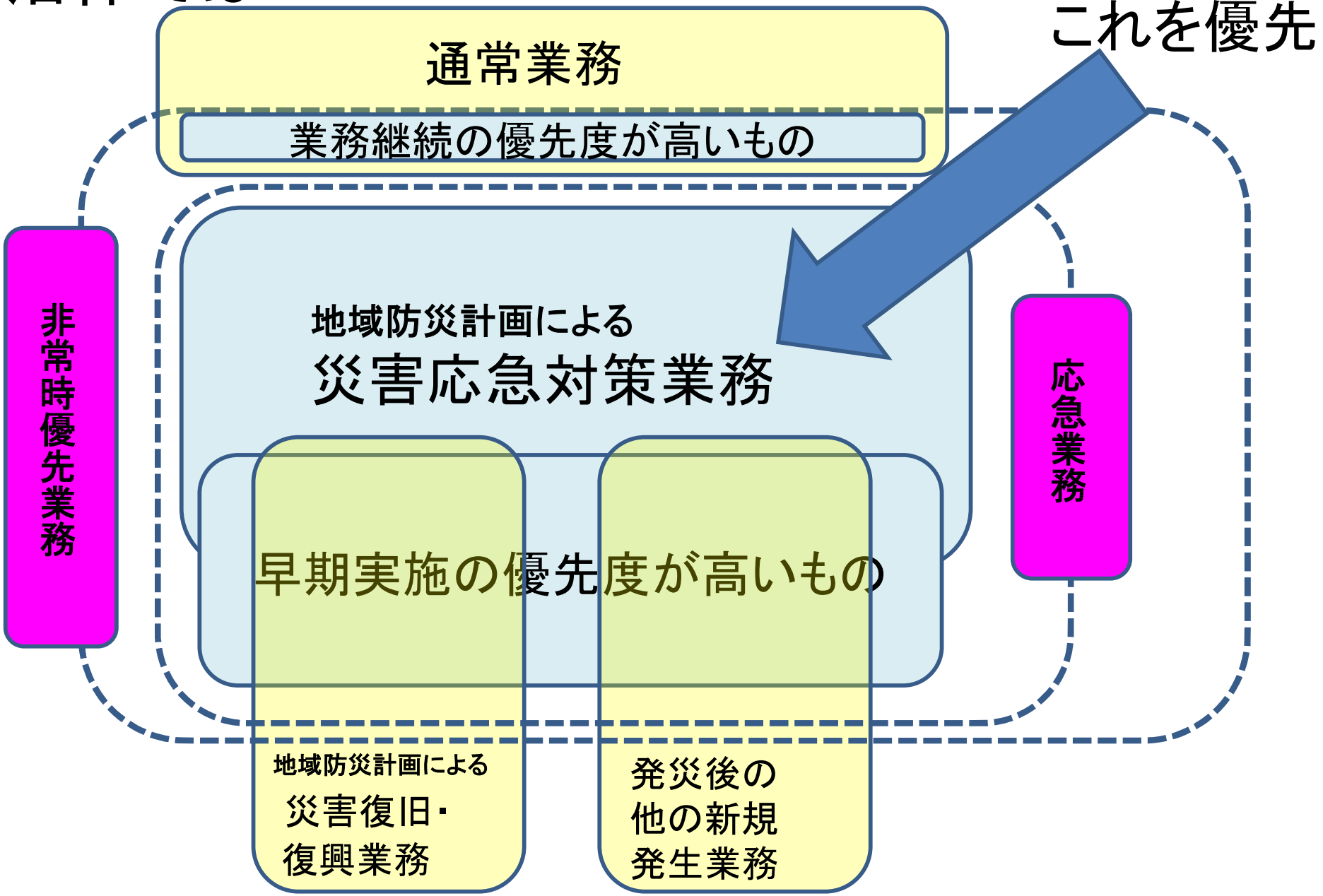
「壊れないように対策する」に「壊れてもいいように対策する」を組み合わせる




＋７２時間
初動
＋１週間
復旧
＋１カ月
復興へ
【図 1-1】復旧曲線
災害発生
通信　２週間
応援　１週間
業務継続実践後の復旧曲線
稼働率
100%
電源　３日間
いかにして
早急に復旧させるか
②
現状の予想復旧曲線
①
いかにして業務を中断させないか
時間

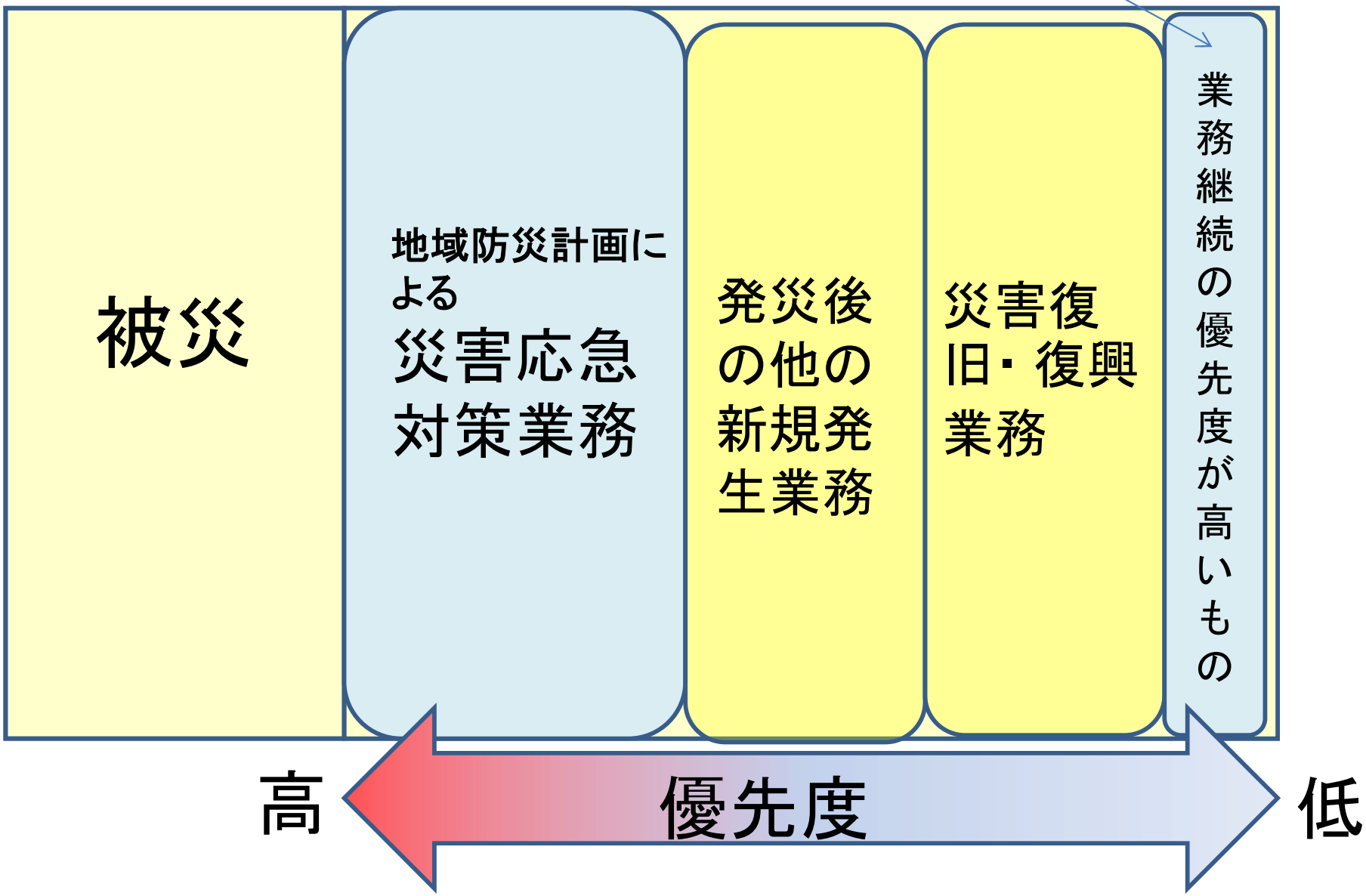

被害の想定
当該部門に該当する被害の想定
実施する対策
残存する被害（受容した被害）
対策レベルを決定する
これは政策判断

自治体では・・・



被災により発生する新たな災害応急業務を実現するための計画である

日常生活を営む市民もいる。通常の業務を求める市民もいる。



だから、業務継続計画ではなく、「業務縮小計画」

BCP

Business Continuity Plan

被災時行動計画

災害や事故などの不測の緊急事態が発生した場合に、事業資産の損失を最小限にとどめ、最低限の事業活動を継続できるよう策定される行動計画

手順書は別個に作成する

事前対策計画（実施計画）

すべてが即時に達成できるわけがない
年度計画を策定して着実に実施する。

BCPで重要なことは、これを推進するため「1年間の間にいつ、何をするか」。そして、それを達成できなければ「来年、再来年にはいつ、何をするか」といった実施計画を策定すること。

もっとも重要な「人」の確保

しかし、防災計画では無視されている・・・

職員呼集 ―― 職員呼集
自動呼集でいいか？

職員（家族）安否確認（システム）

TOP

災対本部員・事務局員等

IT担当職員 → 復旧要員は確保できたか？
誰でもできる？

一般職員

ベンダーの要員の呼集

しかしベンダーも被災しているし、ユーザーは多い。交通遮断。

情報システムの復旧優先度

被災から＋３日まで、＋１週間まで、を想定してみる。
どこまで許容されるか。　＋（　）時間

第１STEP　　災対本部の立ち上げ

物理的なネットワーク

共通基盤

「非常呼集」システム
「安否確認」システム

第２STEP　　「グループウエア」
「ホームページ」

ホームページでメッセージ（第１報）
市長のメッセージ

第３STEP　　「被災者支援システム」（住民基本台帳・GIS）

生活支援・物流支援・・・

そのあとで業務アプリ

（事前）対策の
実施を想定

壊れないように・・・・

庁舎・・・・・・執務空間　代替施設を確保

電源・・・・・・自家発電

代替品・予備機がないもの

メインフレーム（代替品がない）

免震構造の建物　免震テーブル

壊れてもいい、迅速に回復できれば・・・

データ　バックアップ

代替品の確保（どこでも売っている）

（特殊なものを使わない）

予備機がある・バックアップがある

（仮想化、コピーだけ）

クリーンデスクなど

自力で対策できない

通信手段　・・・・・携帯電話、無線

上水、下水、ガス、物流、・・・・

壊れないように・・・・　失ってはならないもの

庁舎・・・・・・執務空間　代替施設を確保
免震構造の建物

電源・・・・・・自家発電　代替施設を確保

免震テーブル

代替品・予備機がないもの

1．メインフレーム（代替品がない）

立ち入り禁止でサーバ等を
引き出せないことも

2．記録された情報が失われる

データ　（バックアップ）・各種設定情報

パソコンに保存された情報は？　回復不可能

紙の情報は散逸、復旧に労力と時間がかかる

壊れてもいい、迅速に回復できれば・・・　（BCPから情報システムを見る）

復旧作業を簡易にする方法

1. どこにでもあるものを使用する。
　　メインフレームから「どこにでもあるサーバ」へ

2. 仮想化　（サーバごとバックアップ、機種に依拠しない）

　転倒防止　免震テーブル・・転倒防止ラック

3. バックアップ保管場所（遠隔地？ネット？いつ届く？）

4. ネットワーク機器類・・・フラットなネットワーク
　　SW類の設定はシンプルに
　　設定情報をバックアップ
　　SW類は固定する
　　無線？
5. クライアント類・・・・・・・・クライアントに情報を蓄積しない

　サーバ室内だけではない

　　各課に配置のパソコンは落下・下敷きに・・
　　たぶんプリンターは落下し壊れるだろう

容易な復旧

「壊れないように対策する」・「壊れてもいいように対策する」

復旧作業を簡易にする方法

メインフレームから「どこにでもあるサーバ」
VMでサーバごとバックアップ
機種に依拠しない手法

どこにでもあるものを使用する。

VM化　（サーバごとバックアップ、機種に依拠しない）

データのバックアップ保管場所（遠隔地？ネット？いつ届く？）

ネットワーク機器類・・・フラットなネットワーク
クライアント類・・・・・・・・クライアントに情報を蓄積しない

要員確保が困難・・・・情報政策課OBを割り当て
誰もが「ここまではできる」　　初動（第2段階）までは誰もができること

➡ 人材養成計画へ

メインフレームは倒壊しない対策を行う

ソフトウェア

特殊なものは使わない

BCPから情報セキュリティを見る

１．組織的・人的なセキュリティは機能しない

「組織」は機能しない。みんな忙しい。　非常時はルールなし。

パソコンや紙情報が散乱・放置されている・・・・

パソコンが盗難にあった。監視下に置けなくなる。

２．物理的・技術的セキュリティが復旧の支障とならないか

被災直後の復旧時にセキュリティは必要か？人命最優先！

セキュリティシステムの障害でネットワークが使えない
１か所集中型は被災しやすい、しかし復旧しやすい

アクセス制御機構が被災　　復旧は容易か

シンクライアント

サーバと接続しなければ使えない、ならば被災直後には使えない。
せめて、ワードとエクセルはうごかしたい。

３．非常時にも有効な技術的セキュリティ

４．非常時にも有効な技術的セキュリティ

インターネットから内部システムへの接続　（簡易な認証）

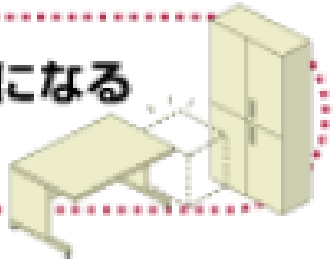
BCPから情報セキュリティを見る

- 人命が最優先、プライバシーは後退する
  - どこまで後退してもいいのだろう・・・・
- 一旦インターネットに表示すれば、取り消しができない（誰かが取り込んでいる）
  - どこまで容認されるのだろう・・・・

自らのプライバシーを犠牲にしてでも安否確認

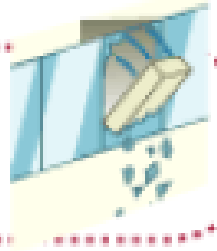
Ⓐ 避難経路の幅は１ 2m以上ある

Ⓑ 通路付近に避難の障害になる
物は置いていない

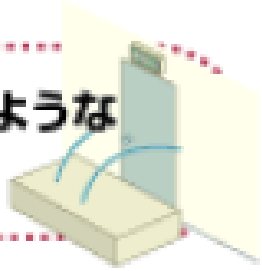


Ⓒ 避難経路・避難方向は
明確になっている

Ⓓ 窓付近に背の高い家具を
置いていない



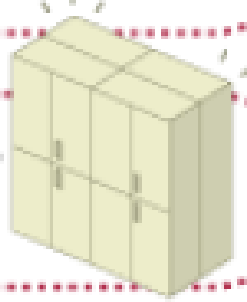
Ⓔ 避難経路に転倒・移動するような
家具・什器は置いていない



Ⓕ 金庫など重量のある家具・什器
は適切な位置に設置している

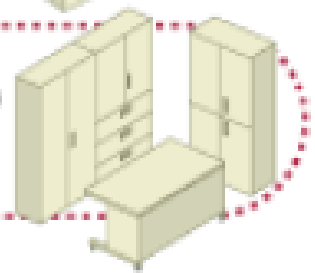
Ⓖ 床は避難の際すべりにくく
転んでもケガしにくい材質である

Ⓗ オフィス内で収納家具を
単体で設置していない



Ⓘ ガラス扉のついた
家具・什器は置いていない

Ⓙ デスクまわりに背の高い
家具を置いていない



壊れてもいい、迅速に回復できれば・・・

日常業務の中のBCPという視点

1. 人命が失われる

   業務中だったら事務機器が凶器となる。 → 固定

2. 人の記憶が失われる

   担当者がケガで入院、代替要員で継続可能？ → 情報共有

3. 記録された情報が失われる

   紙の情報は散逸、復旧に労力と時間がかかる → 整理整頓

   パソコンに保存された情報は？　回復不可能・・・ → PCに保存しない

4. 執務空間が失われる

   庁舎倒壊

   設備使用不能（上水・下水・電源）

   散乱 → 固定 整理整頓

5. 機器類の機能が失われる

   損壊する

「想定以上の津波が来た。想定以上の地震だった。」

「津波が５～６メートルの高さであれば施設の安全性は保てる

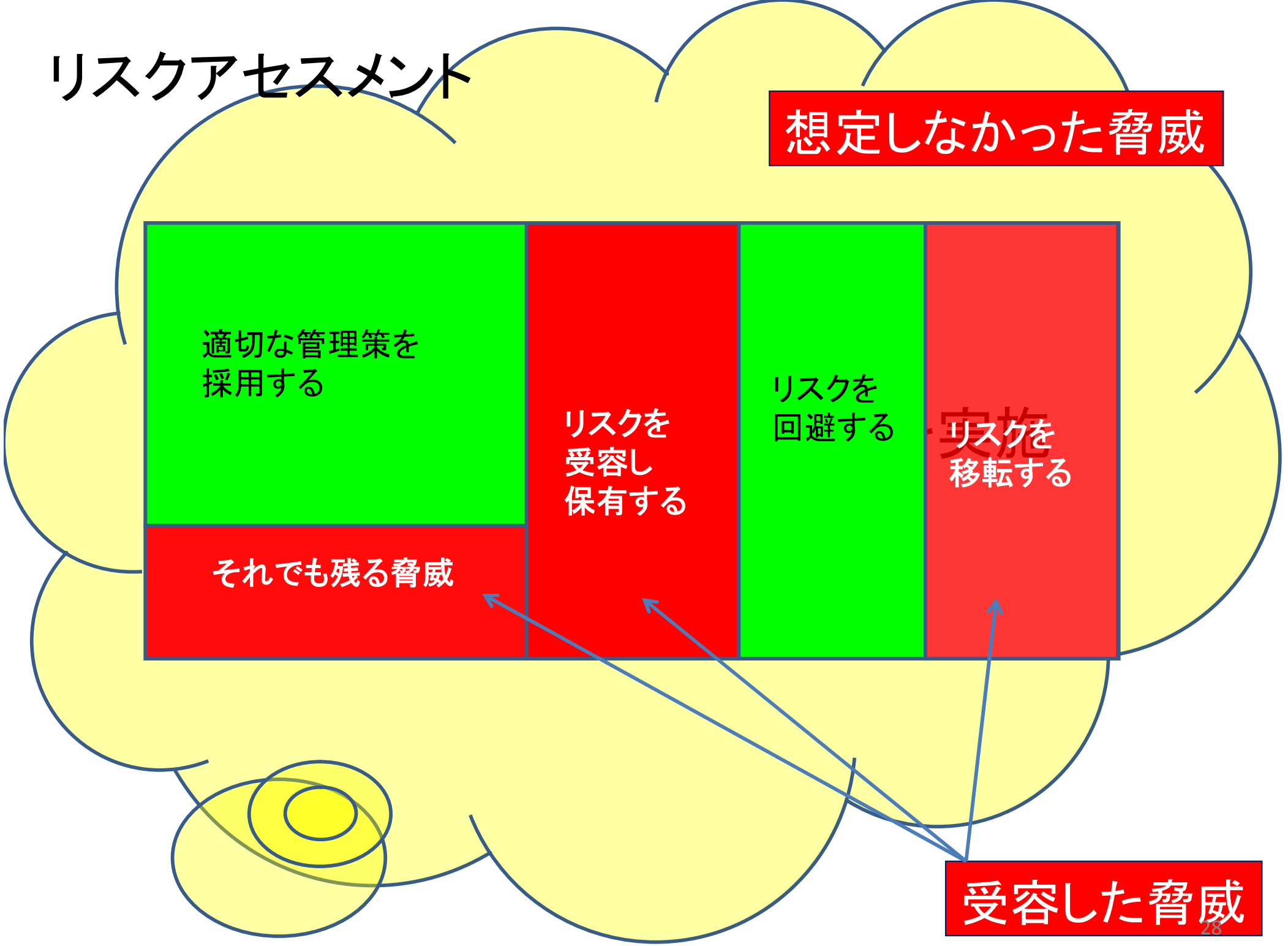
福島第一、第二原子力発電所周辺を襲った津波は、想定を超える14メートル以上だった・・・

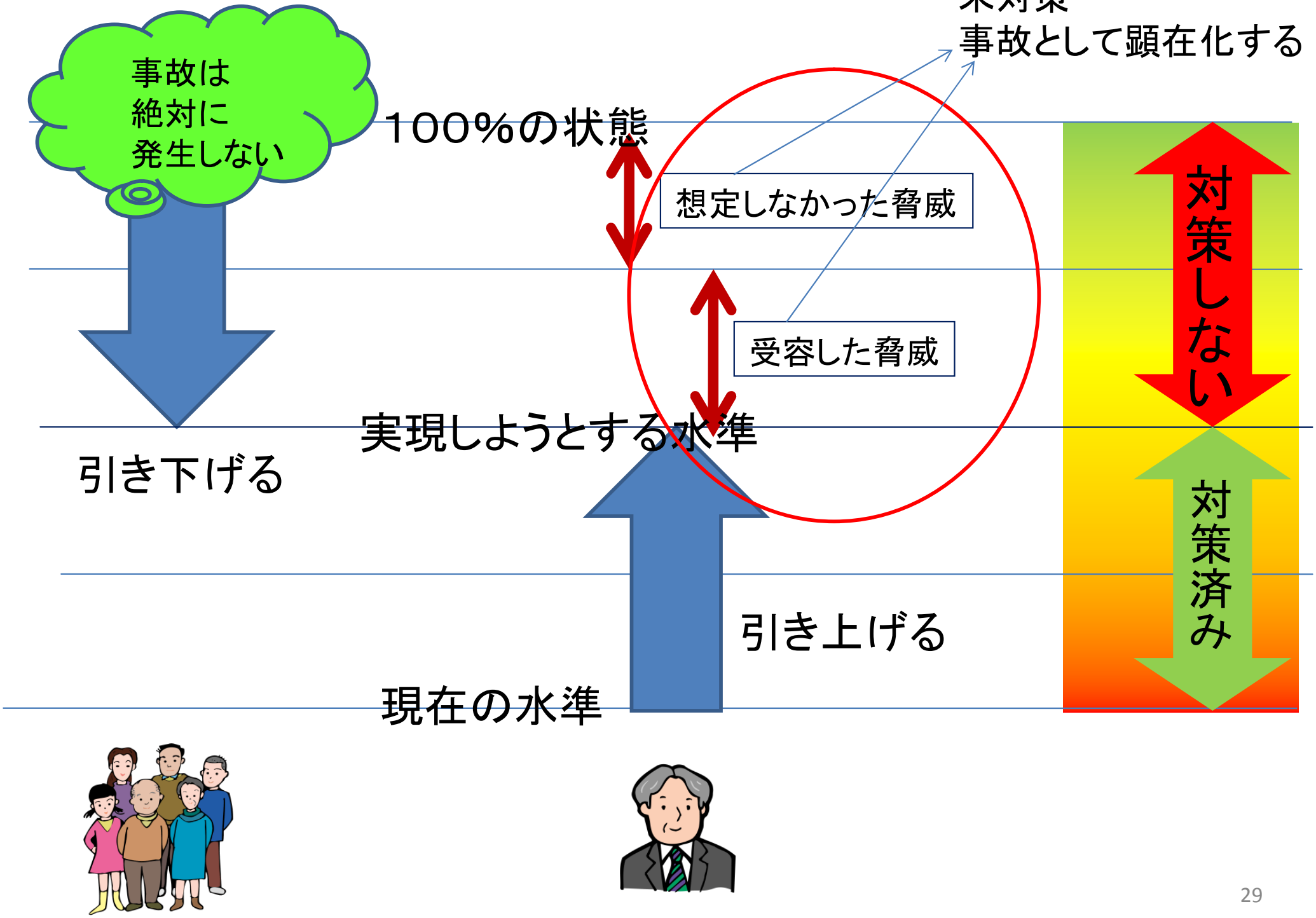
近海でマグニチュード（Ｍ）８・０の地震による津波で水位が上がっても、海水ポンプなどの機器に「影響はない」としていた。

今回の地震の規模はＭ９・０で、想定した地震の約３０倍というけた違いの大きさ。

この「想定」を住民に伝えず、「安全！」といっていた。 騙された！

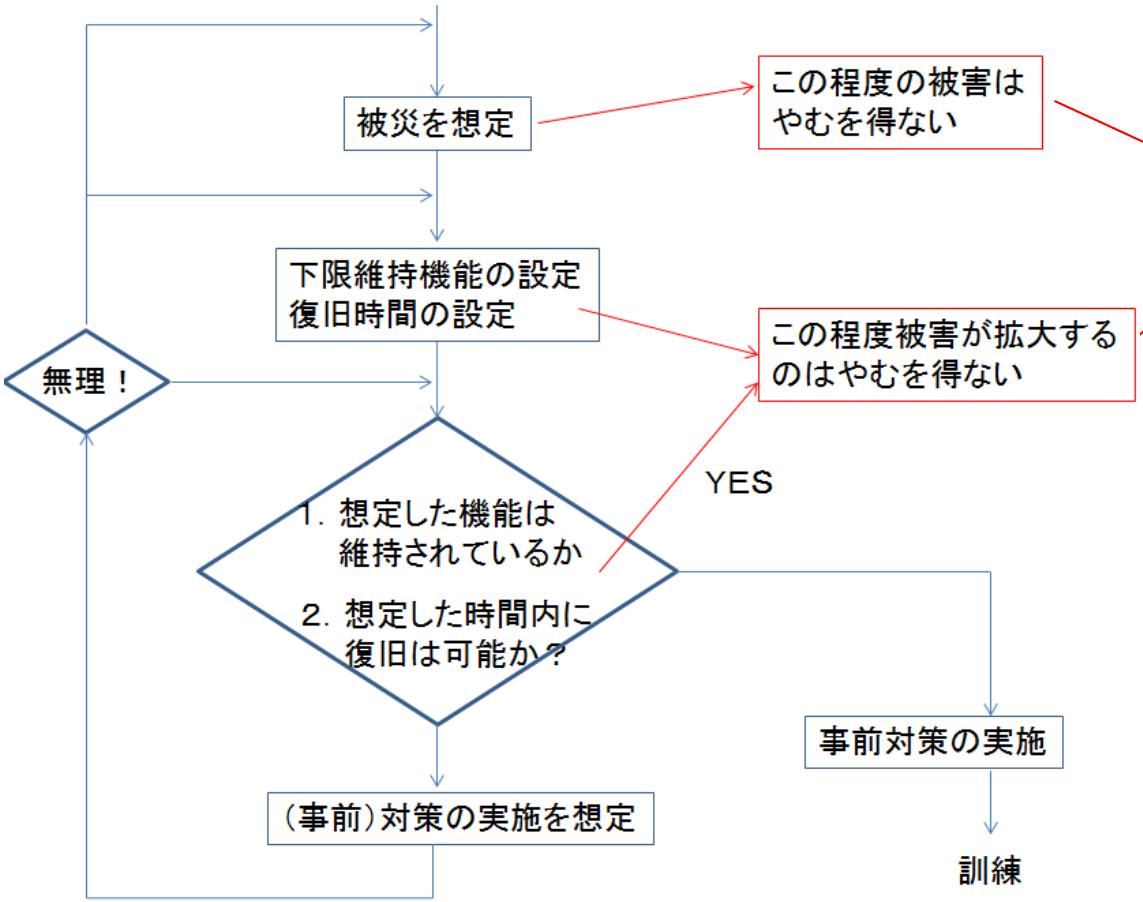
リスクアセスメント


想定しなかった脅威
適切な管理策を
採用する
それでも残る脅威
リスクを
受容し
保有する
リスクを
回避する
リスクを
移転する
受容した脅威


未対策
事故として顕在化する
事故は
絶対に
発生しない
100%の状態
想定しなかった脅威
受容した脅威
対策しない
実現しようとする水準
引き下げる
対策済み
引き上げる
現在の水準

ここで「受容した脅威」は「受容した被害」である。
「想定しなかった脅威」も同様。

「受容した被害」が具体的な「被害」として顕在化する。



この程度の被害は
やむを得ないと受容すると決定

地域防災計画では全力投入
BCPでは・・・

自治体では・・・
企業では・・・

リスクコミュニケーション

加害者と被害者のリスクコミュニケーション

開示が必要なのは、「想定」と「受容したリスク」

危険を告知する・合意する

タバコ
喫煙は、あなたにとって脳卒中の危険性を高めます。
疫学的な統計によると、喫煙者は脳卒中により死亡する危険性が非喫煙者に比べて約１．７倍高くなります。

人により程度は異なりますが、ニコチンにより喫煙への依存が生じます。

インフォームドコンセント**informed consent**
特に、医療行為（投薬・手術・検査など）や治験などの対象者（患者や被験者）が、治療や臨床試験・治験の内容についてよく説明を受け理解した上で (informed)、方針に合意する (consent) ことである。説明の内容としては、対象となる行為の名称・内容・期待されている結果のみではなく、代替治療、副作用や成功率、費用、予後までも含んだ正確な情報が与えられることが望まれている。

おしまいです