リスクマネジメントと危機管理
～想定内と想定外：
原点に戻って考える～

立教大学大学院21世紀社会デザイン研究科
客員教授
博士（情報学）、システム監査技術者、気象予報士

指田　朝久

1．日本での用語：危機管理：

●危機管理：不測の事態に対して事前に準備される、被害を最小限に食い止めるための対策　（クライシスマネジメント）

リスクマネジメントを含む概念であり、「危機管理」として使用される場合にこれらのいずれを指すか、または両方を含んでいるかは少し曖昧である

出典：大辞林第三版

○クライシス（crisis）：危機、重大局面、決定的段階、転機；
金融危機、食料危機

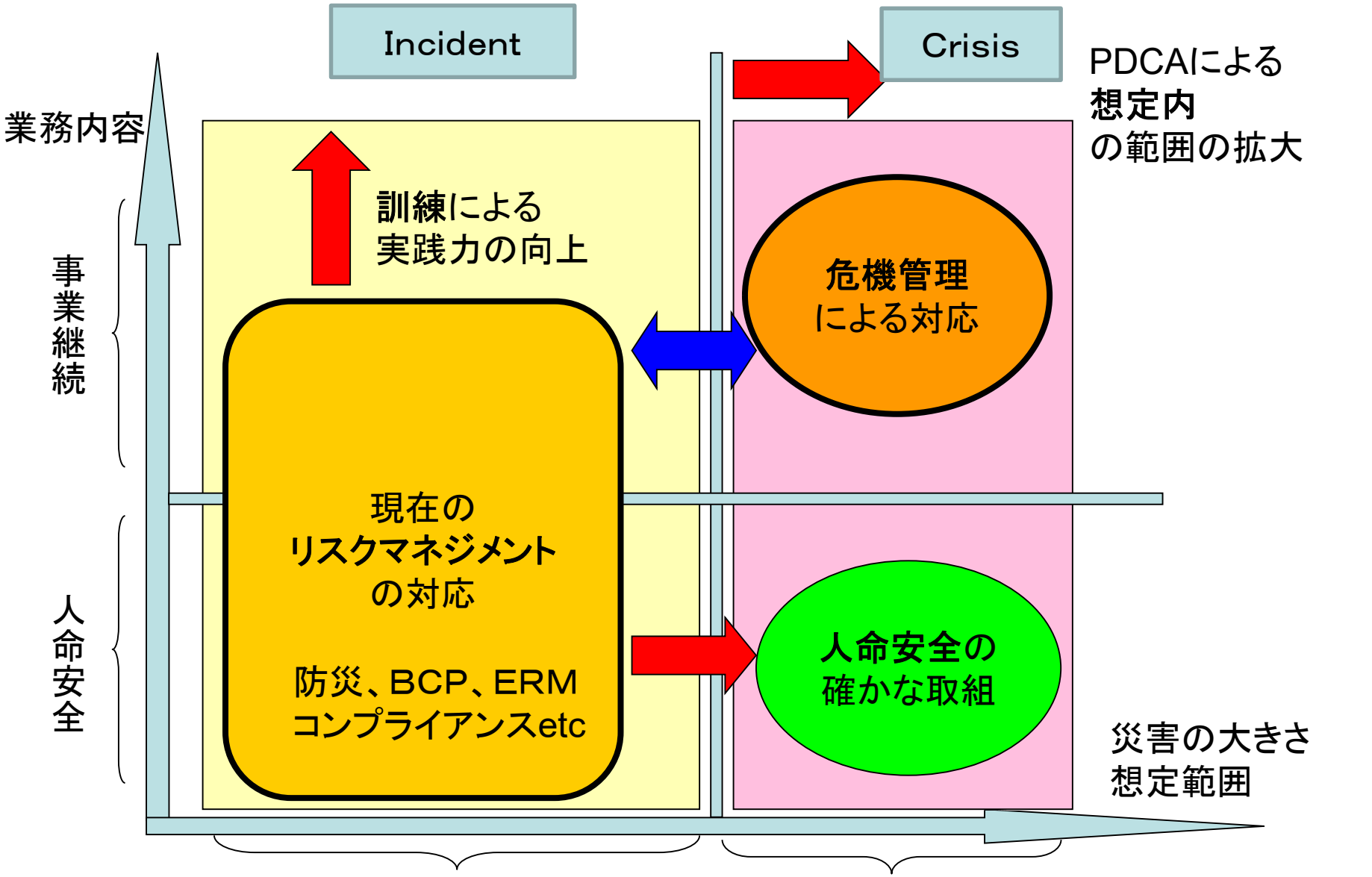
出典：プログレッシブ英和辞典第4版

日本での用語「危機」の使われ方

- 生死にかかわる問題：交通事故、入院、疫病など
- 家庭の破滅、一家離散などへの直面；破産など
- 防災、防犯、テロ対策（駐在員の誘拐対策）；
  地震、火災、誘拐など
- 組織の崩壊、解散

など

2. 想定内と想定外;東日本大震災の教訓



出典:リスクマネジメントが
よ~くわかる本第二版　4

危機と災害対応

- 危機に対応する英語

Incident < Emergency <<< Crisis < Disaster <Catastrophe

起きてしまった事の程度によって、言葉が変わる

（出典：林春男, 牧紀男, 田村圭子, 井ノ口宗茂；組織の危機管理入門リスクにどう立ち向かえばいいのか；丸善；2008）

被害**想定内**の出来事　　Incident 、Emergency

想定外および想定以上の出来事　Crisis 、Disaster、Catastrophe

日本語

事案、事件、事故、緊急事態、危機、災害、破局、出来事・・・

想定内の対応においても災害対策本部と言っている

（日本語の「災害」は英語の“Disaster”と対応しない）

危機管理とCrisis

★日本語の「危機（管理）」と英語のCrisisは1対1に対応しない
3種類の意味がある。

①日本語の「危機（管理）」は英語のCrisis加えて、
テロ、犯罪、絶体絶命などの命に関わるものについて
事前準備、起きた後のIncident対応のニュアンスを含む
つまり **Security** の概念を含んでいる

②日本語の「危機（管理）」は英語の Crisis および Incident の
事後対応に加えて Incident に対する事前準備も含む
英語ではIncident Preparedness（準備）があたる

マスコミが「危機管理ができてない」という場合はIncident Preparedness
ができていないという意味で用いられることが多い

（出典 指田朝久(2016),日本の災害対策に必要な事案管理と危機管理の概念整理,地域安全学会梗概集No37）

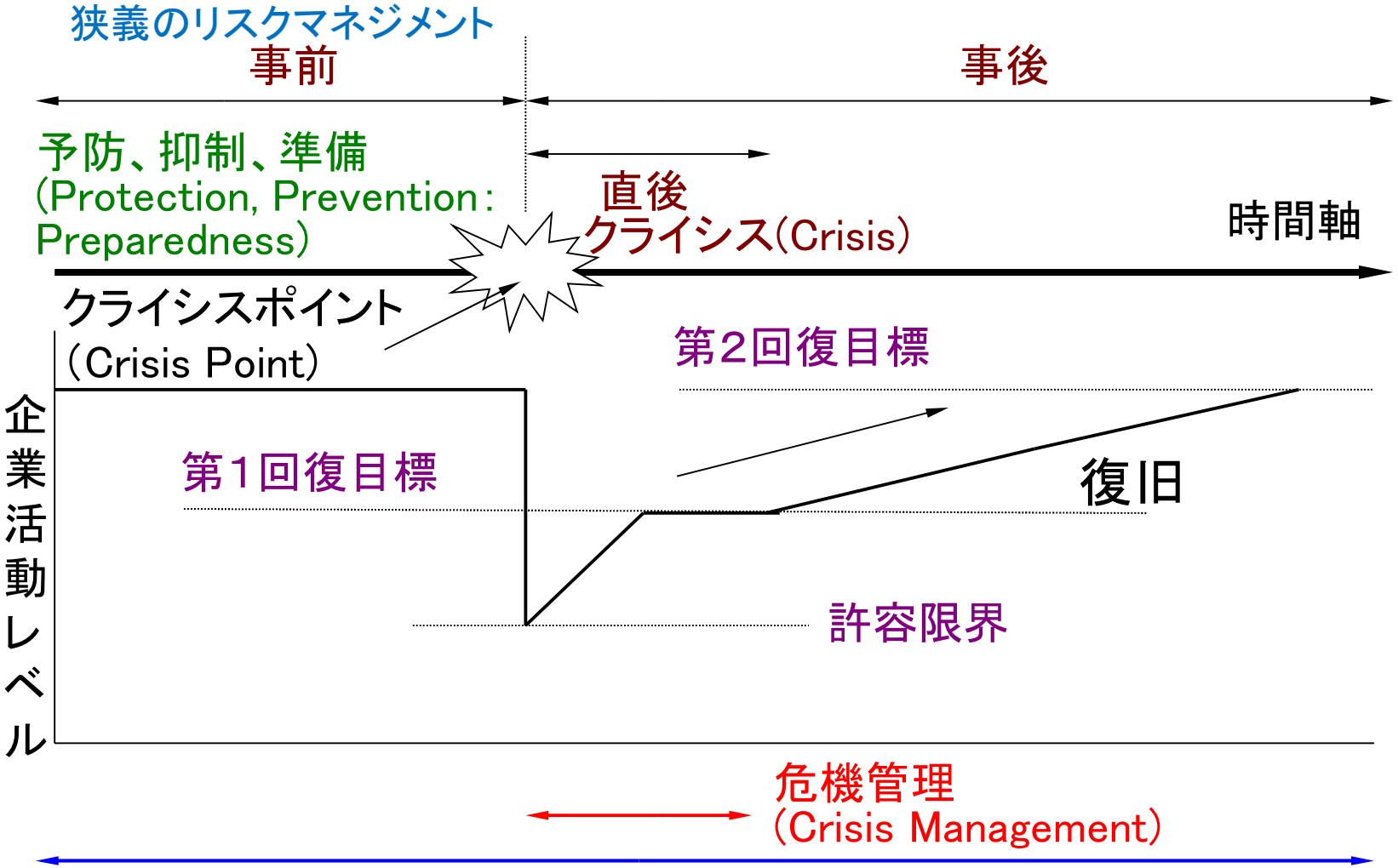
3．リスクマネジメントと危機管理

- 阪神・淡路大震災の教訓を活かしたJISQ2001（リスクマネジメントシステム構築のための指針）の制定

①事前の予防策（狭義のリスクマネジメント）、
②事件事故（クライシス）発生直後の対応（危機管理）、
③復旧の3つの時間軸に沿った対応
のすべてを含む概念として
広義の「リスクマネジメント」を定義した

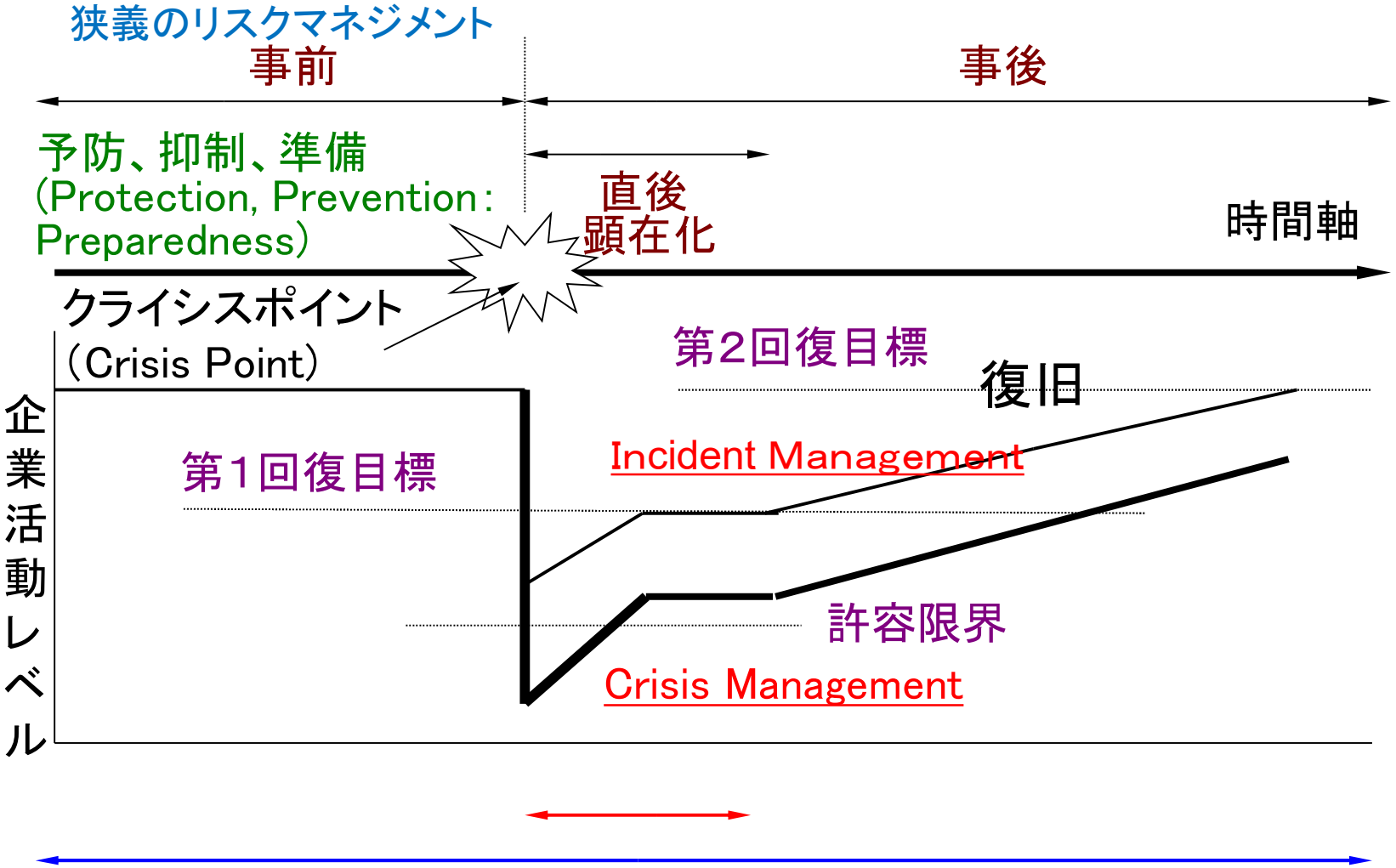
ただし、正しくは本来は事前に備えIncidentで済ますべきものが、対応できておらず危機管理Crisisとなったため、事後対応のすべてが危機管理の概念として考えられていたと思われる。(指田）

言葉の定義（JISQ2001）



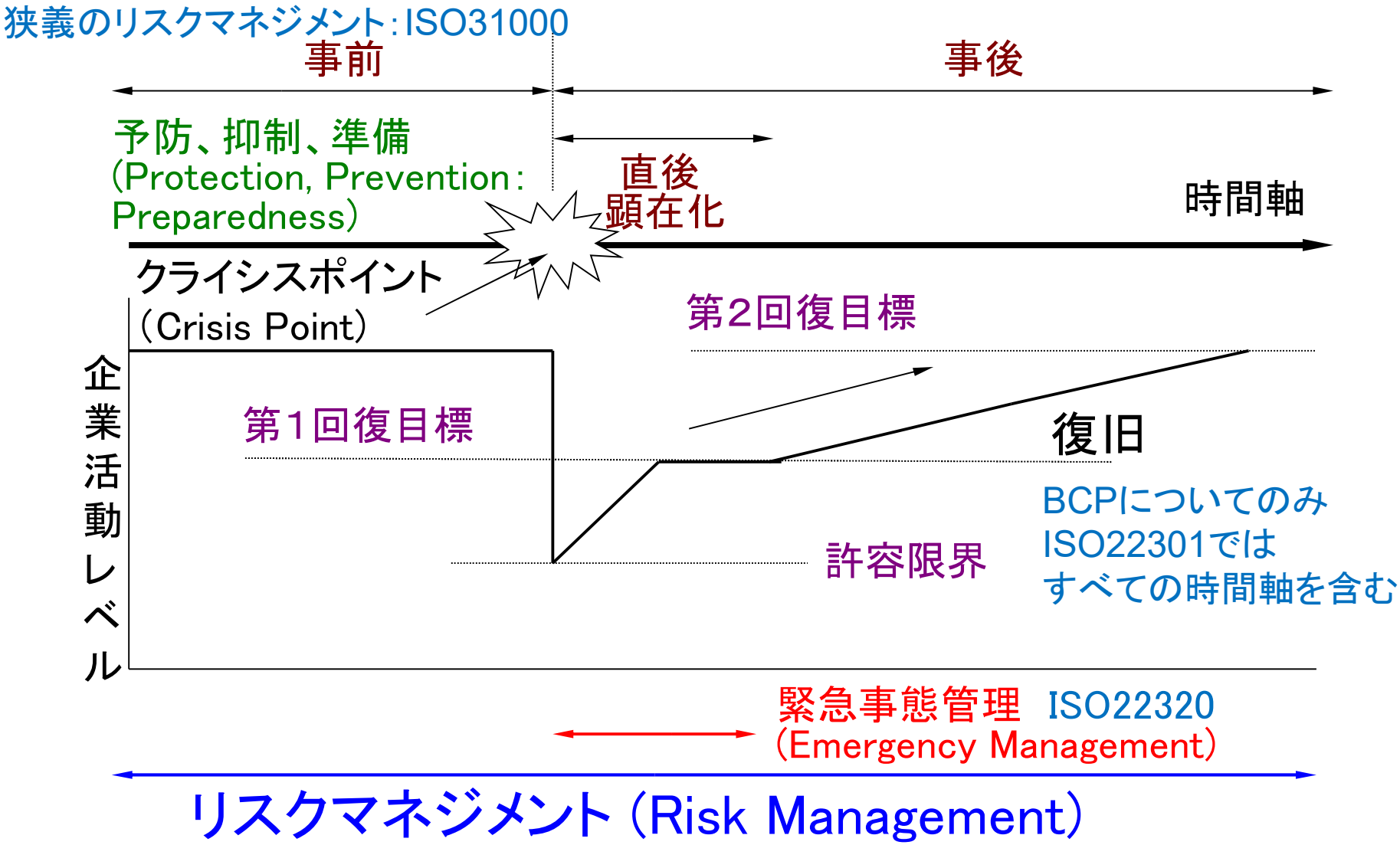
出典： JISTRZ0001（JISQ2001の原案）に加筆

言葉の定義（正しくは）



出典： JISTRZ0001（JISQ2001の原案）に加筆

言葉の定義（ISOの世界）



出典：　JISTRZ0001（JISQ2001の原案）に加筆

ISOの世界の分担

規格番号	規格名称	内容
ISO31000	リスクマンジメント ー原則及び指針	日常の活動が対象 予防、抑制、軽減、準備など
ISO22320 ※	社会セキュリティ ー緊急事態管理 ー危機対応に関する要求事項	あらかじめ想定される事件や事故発生時の組織や情報収集・整理・行動要領など 政府や公的組織の応援、協調などを想定
ISO22301	社会セキュリティ ー事業継続マネジメントシステム ー要求事項	BCPについて、日常の組織活動のPDCAをはじめ、万が一事業継続計画の発動後の組織活動の要領および復旧にむけた取り組みなど時間軸のすべてを規定

※ISO22320は英語名が
Emergency Management－ Requirements for Incident response
であり、想定内の領域を対象としている。（危機対応という訳語は好ましくないと考える）
想定外や想定を超えたCrisis にあたる対応を定めたISO規格はまだない。

おすすめの用語の使い分け

- リスクマネジメント；日常の予防、リスクが顕在化した場合の対応、および復旧のすべての活動を含む；広義で用いる。この場合のリスクが顕在化した場合には①想定内で対応可能（Incident)、②想定内のリスクが手に負えなった、想定外および想定以上（Crisis)の両方の対応を含む
  Incidentなどが発生した場合の事前の備えPreparednessを含む

- 事案対応（Incident対応）；想定したリスクが顕在化したが、あらかじめ想定される当該リスク対応策（対策マニュアルの構築）で対応できるもの
  （想定外のリスクが顕在化したが程度が小さく日常対応の延長線上で
  対応できるものも含む）

- 危機管理（Crisis対応）；想定したリスクが顕在化したが、被害程度が当該リスク対応策で対応できない規模、あるいは対応に失敗した場合、および想定外のリスクが顕在化し被害程度が甚大なもの

いわゆる危機管理マニュアルは「事案対応マニュアル」となるべき

危機管理;Crisis　Management

★基本的には想定外の対応であるため、何等かの被害は避けられない
★既存の構築されている何等か類似のリスク対応策を応用して対処する
★基本的にはトップダウンで意思決定する
★対応策はプロシージャー（チェックリスト）で管理は可能
★意思決定する個人および、情報などを整理する組織の応用力が試される

＜＜プロシージャーの例＞＞
①ゴールは何か
②原因は何か
③対処策は何か（必ず代替策と比較する）
④対策の進捗状況をどう確認するか
⑤対応策が成功した場合の残るリスクは何か

事案対応マニュアルにチェックリストを追加して入れておけばよい
（　注　イギリス規格BS11200：Crisis Managementが策定された）

4. リスクについて:最新の言葉の定義

- 言葉の定義:国際標準規格ISO31000「リスクマネジメント―原則及び指針」と会社法362条の違い

リスク;**目的に対する不確かさの影響(ISO31000)**

Risk: Effect of uncertainty on objectives

リスク:**目的の達成を阻害する要因(会社法)**

リスクマネジメント;リスクについて組織を指揮統制するための調整された活動(ISO31000)

リスクマネジメント;損失の危険の管理(会社法)

ISO31000のリスクの定義

● ISO31000 ;2018 国際標準規格リスクマネジメント一指針

RISK; effect of uncertainty on objectives

目的に対する不確かさの影響

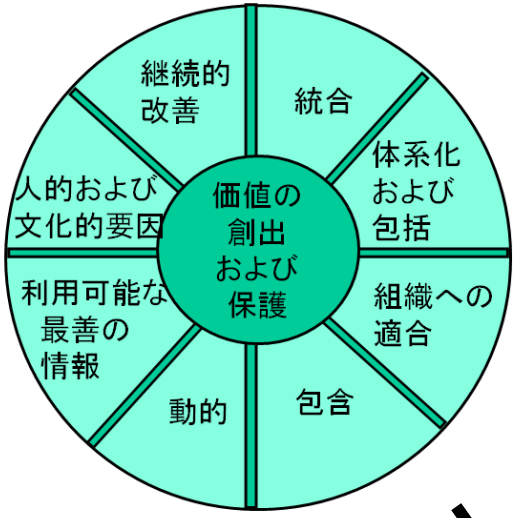
・NOTE1 影響とは、期待されていることから乖離することをいう。
影響には好ましいもの、好ましくないもの、またはその両方の場合があり得る。
影響は、機会または脅威を示したり、創り出したり、もたらしたりすることがあり得る。

・NOTE2 目的とは、様々な側面及び分野をもつことがある。また、様々なレベルで適用されることがある。

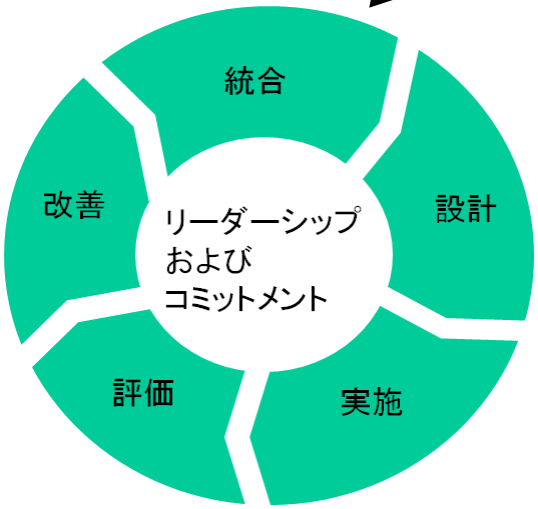
・NOTE3 一般に、リスクは、リスク源、起こり得る事象、及びそれらの結果、並びに起こりやすさとして表される

注 ISO31000では金融工学のリスクの定義も取り込んで定義された。
金融工学ではリスクとリターンの組み合わせが一般的に用いられており、金融工学のリスクの定義ではリスクはプラスの値をとり悪いものを意味するものではない。

ISO31000:2018改訂の概念図



原則　4章



枠組み　5章

プロセス　6章

５．ISOで統一されたマネジメントシステムの項目

０．序文
１．適用範囲
２．引用規格
３．用語および定義
４．組織の状況
５．リーダーシップ（方針、組織の役割、責任権限）
６．計画
７．支援（資源、力量、認識、文書化した情報、文書管理）
８．運用
９．パフォーマンス評価（監視、監査、マネジメントレビュー）
１０．改善

分野固有の要求事項は6．または8．に記載（または付属書）
ISMS：ISO27001も今回の改定で統一された記述を取り入れた

統一されたマネジメントシステムの中の用語の混乱

統一されたマネジメントシステムでは

なんらかの対応を行う場合に必ずリスクアセスメントを実施することを要求しており、ISO31000のリスクマネジメントプロセスを実施する。

ところが

この中でリスク(risk）と機会（Opportunity)を分析することを求めている。これはrisk　をマイナスと捉えていることになる

一方ISO31000の　risk　はプラスマイナス両方を含む概念である

このように現在のISOは一部に認識の混乱が存在する。

組織内部での用語の使い方とISO

ISOの言葉の定義は、現在様々なISOの規格の中で用いられている様々なニュアンスの一番広い、合意ができる範囲での用語の定義を行う。

従って、各自各組織の用語の使い方において、限定して定義をして用いることは問題ない。

実際に”Risk“はISOではプラスマイナス両方を含む（あるいは中立な）定義であるが、会社の実務においては、戦略リスクや財務リスクなどプラスマイナス不可分のものも含めて対処しており、かつ、実務的には会社経営の存続にかかわるマイナスの部分に着目してマネジメントする場合が多い。

マネジメントシステムの統合においても、ISO31000のリスクの定義よりも限定した、マイナスのみをリスクとして捉えて運用しても全く問題ない

組織内部での用語の使い方とISO－２

Incident と Accident も様々な使い方がある。

一般にIncidentに、実際に顕在化したリスクのみならず、発生が十分予想される未発生の予兆段階のものをIncidentという用語に含むことも多い。

また、Incident を 未発生の段階、 Accident を顕在化したもの と区分して管理している組織もある。

これらは実社会において様々な用語の使用法がされているのでどれが正しいかは一概には決められない。組織内で誤解が無いように徹底する。

組織内部での用語の使い方とISO－３

Incident　に関するISOの定義

JISQ27000 ―セキュリティ技術―情報セキュリティマネジメントシステム―用語

3.31　情報セキュリティインシデント（Information security incident)

望まない単独若しくは一連の情報セキュリティ事象（3.30)、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの

3.30　情報セキュリティ事象（Information security event)

情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス、若しくはネットワークの状態に関連する事象

JISQ22300―社会セキュリティ―用語

2.1.15　インシデント（Incident):中断、阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況