みんなで考えるリスクマネジメント

～こんなに違う組織内でのリスクのとらえ方～

2013/11/27

リスクマネジメント研究分科会

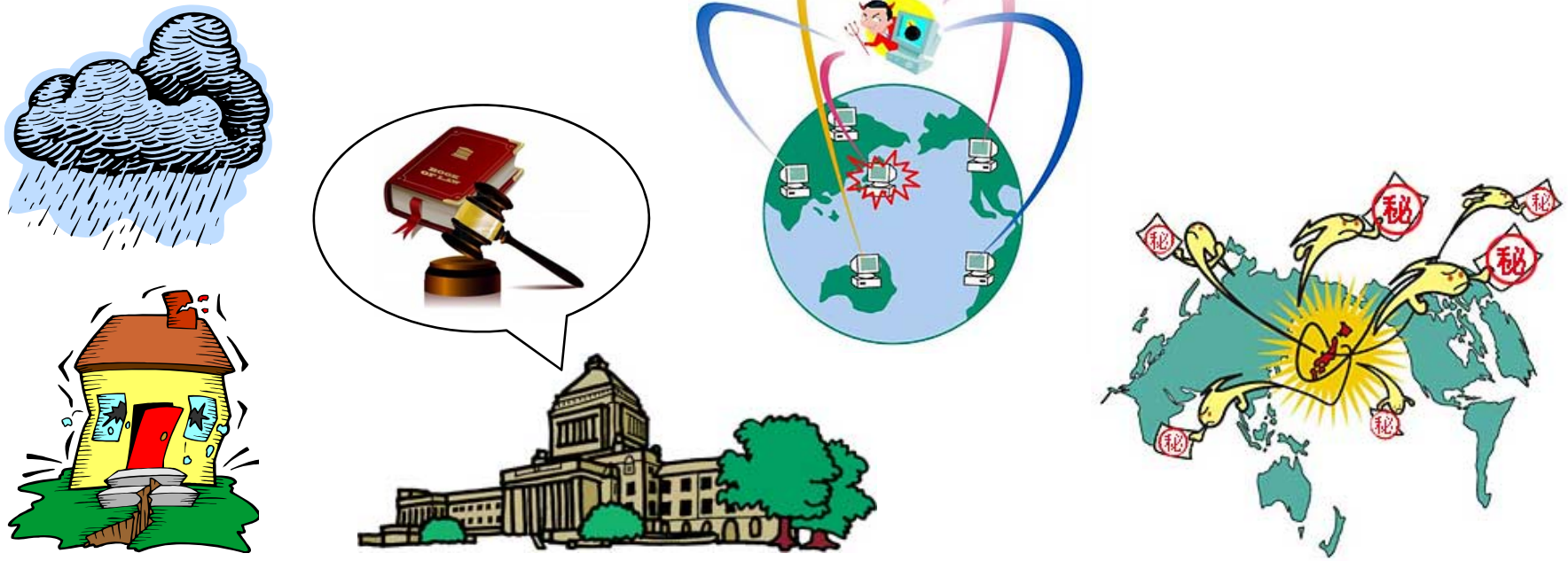
itSMF JAPAN

発表の流れ

1. 分科会の目的・背景
2. リスクマネジメントとは何か？
3. リスクの洗い出し
4. リスクとは何か？
5. リスクマネジメントの課題
6. リスク洗い出しの阻害要因
7. 阻害要因への解決策
8. まとめ
9. 今後の研究予定
10. 分科会紹介

分科会の目的・背景

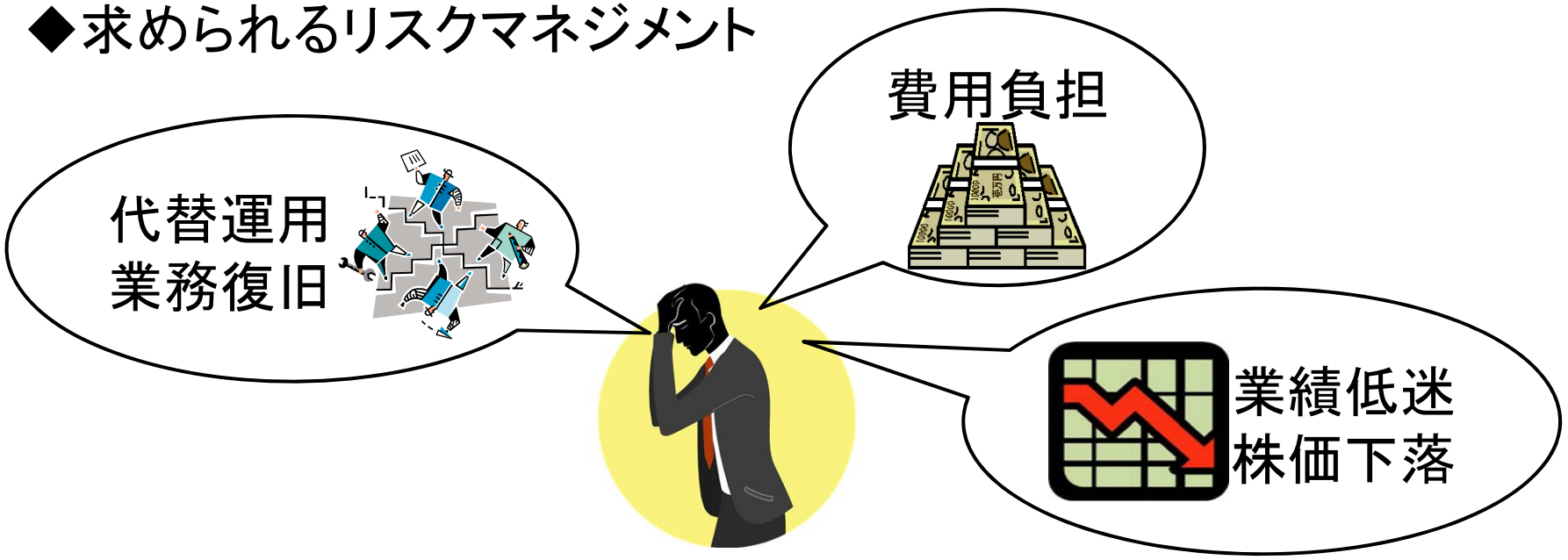
◆求められるリスクマネジメント



震災や水害などの自然災害だけでなく、事件・事故など不測の事態に対応するため、各企業はリスクマネジメントが求められている。

分科会の目的・背景

◆求められるリスクマネジメント



リスクマネジメントは、「企業の損失やダメージを最小限に抑える」ための必要不可欠の要素である。
これを怠ると、企業イメージの低下や存続の危機にも繋がる。

分科会の目的・背景

◆リスクマネジメントに触れているフレームワーク

ISO Guide 73（JIS Q 0073）	リスクマネジメント－用語。2009年発行。
ISO 31000（JIS Q 31000）	リスクマネジメント－原則及び指針。2009年発行。
ISO/IEC 31010（JIS Q 31010）	リスクマネジメント－リスクアセスメント技法。2009年発行。
ISO/IEC 20000-1 （JIS Q 20000-1）	情報技術－サービスマネジメント－第1部：サービスマネジメントシステム要求事項。2011年改版
ISO/IEC 27001（JIS Q 27001）	情報技術－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－要求事項。2013年9月改版。
ISO/IEC 27005	情報技術―セキュリティ技術―情報セキュリティリスクマネジメント。2011年発行。
ISO 22301	社会セキュリティー事業継続マネジメントシステム－要求事項。2012年5月発行

分科会の目的・背景

◆リスクマネジメントに触れているフレームワーク

JIS Q 15001	個人情報保護マネジメントシステム－要求事項。2006年改版
ISO/IEC 15026（JIS X 0134）	システム及びソフトウェアに課せられたリスク抑制の完全性水準。1998年発行。
ISO/IEC 16085（JIS X 0162）	システム及びソフトウェア技術－ライフサイクルプロセス－リスク管理。2006年発行
NIST Special Publication 800-30	米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書。ITシステムのためのリスクマネジメントガイド。
PCIDSS	クレジット業界におけるグローバルセキュリティ基準。2013年10月V3.0が発行。

分科会の目的・背景

◆リスクマネジメントに触れているフレームワーク

PMBOK	アメリカの非営利団体PMIが策定した、モダンプロジェクトマネジメントの知識体系。
COBIT	情報システムコントロール協会（ISACA)とITガバナンス協会（ITGI)がまとめる、情報技術 管理についてのベストプラクティス集。
Risk IT	ISACAの発行するITのリスクの効果的なガバナンスおよび管理のためのフレームワーク。
COSO	1992年に米国のトレッドウェイ委員会組織委員会（COSO）が公表した、内部統制のフレームワーク。
M_o_R	組織が、組織の達成目標に影響を及ぼすリスクについて決定することに対してのフレームワーク。

リスクマネジメントについて触れているフレームワークは、数多く存在する。

分科会の目的・背景

◆ITIL®で言及されている「リスク」

- サービスストラテジ
  - お客さま関係のリスク
  - モニタ活動としてのリスクアセスメント
- サービスデザイン
  - 設計プロジェクトとしてのリスク管理
  - プロアクティブな活動としてのリスクアセスメントとリスク管理
  - 要件と戦略としてのリスクアセスメント
  - 機密性、完全性、可用性のリスクアセスメントとリスクコントロール
  - サプライヤの評価

分科会の目的・背景

◆ITIL®で言及されている「リスク」

- サービストランジション
  - 変更に伴うリスクアセスメント
  - リスク方針に基づく試験
  - 変更に伴うリスクコントロール
- サービスオペレーション
  - オペレーション段階のリスクアセスメントとコントロール
- CSI
  - CSIの取り組みの一部としてのリスクマネジメント

分科会の目的・背景

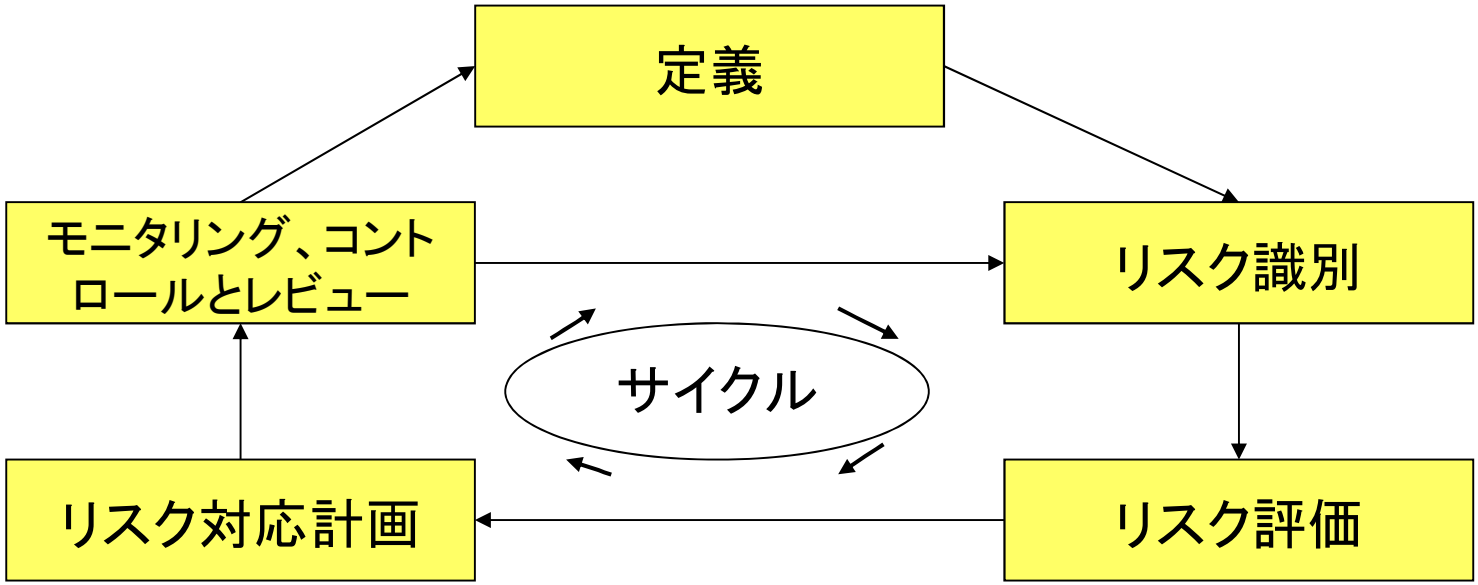
◆ITIL®で言及されている「リスク」

- 共通
  - プラクティスとしてのサービスマネジメント
  - サービスの定義
  - 各プロセスの実装リスク
  - ライフサイクルの各ステージの実装リスク
  - リスクアセスメントとリスク管理

ITIL®でもライフサイクルの色々な段階・プロセスでリスク管理が必要とされているが、具体的な活動は記述されてない。
どのような活動をすれば良いか、気付きを見つける。

リスクマネジメントとは何か？

◆リスクマネジメントの共通的プロセス

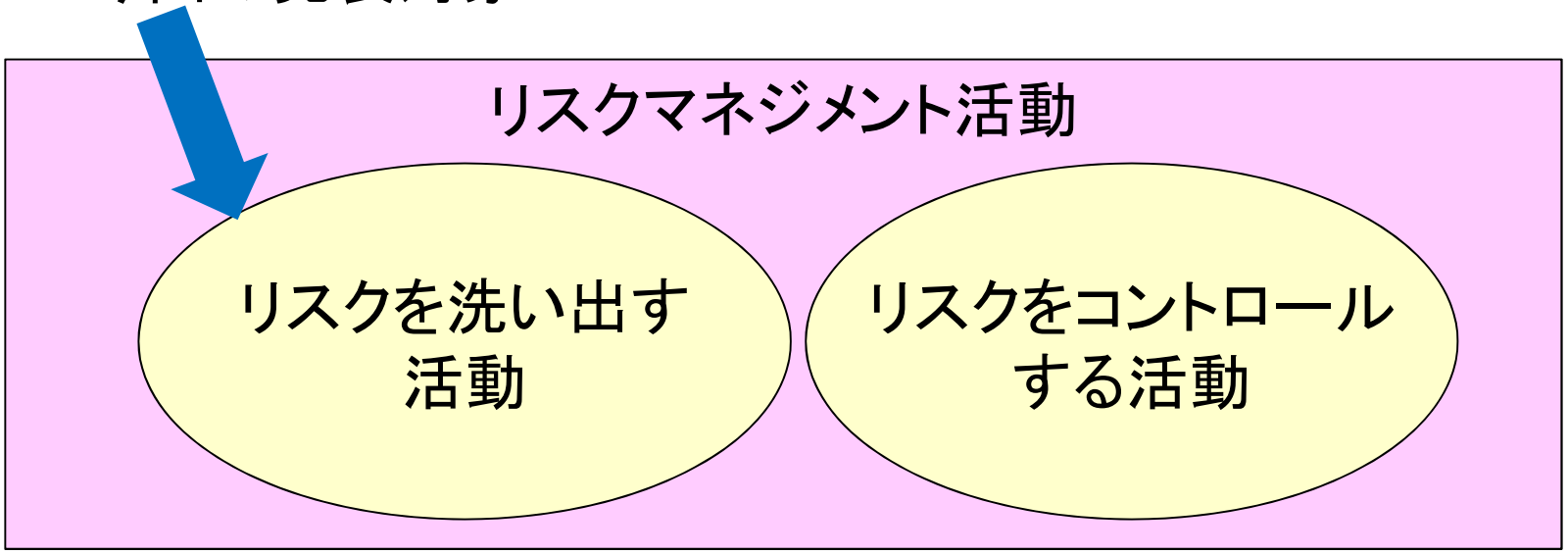


リスクマネジメントに関するフレームワークは数多く存在するが、リスクを定義・識別・分析して、リスク評価の結果を元に、リスク対応を行うプロセスはほぼ同一である。

リスクマネジメントとは何か？

◆リスクマネジメントの活動

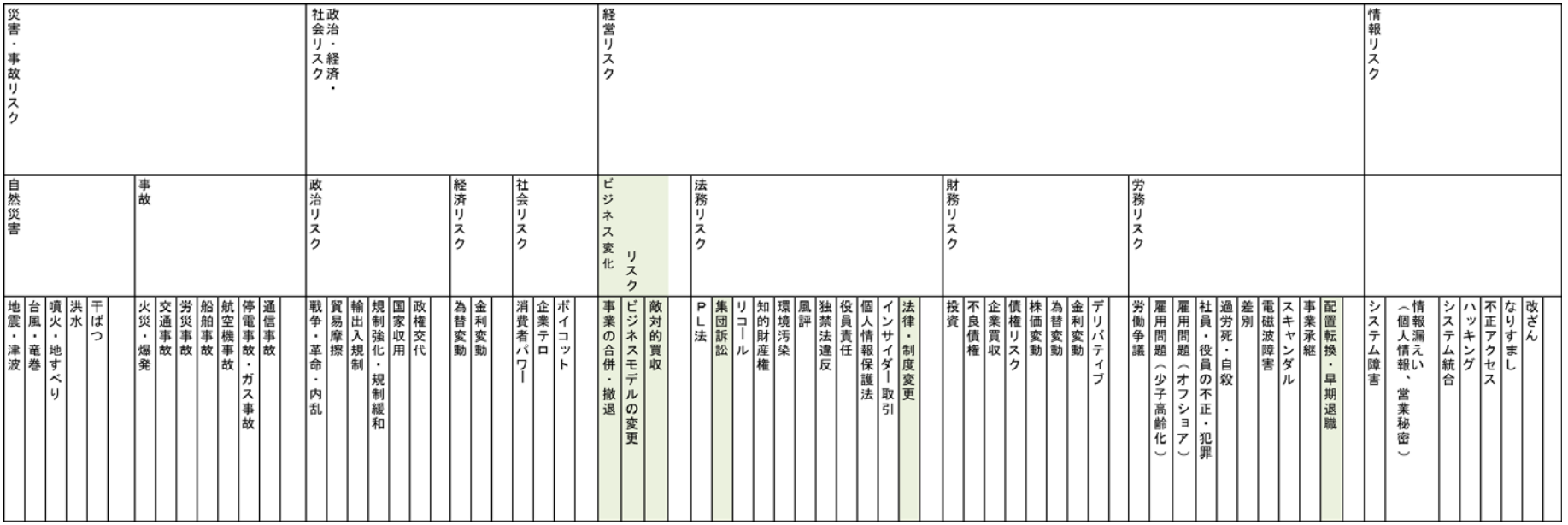
今回の発表対象



リスクマネジメントとは、大きく「リスクを洗い出す活動」と「洗い出したリスクをコントロールする活動」に分かれると考えた。
今回は「リスクを洗い出す活動」の研究成果を発表する。

リスクの洗い出し

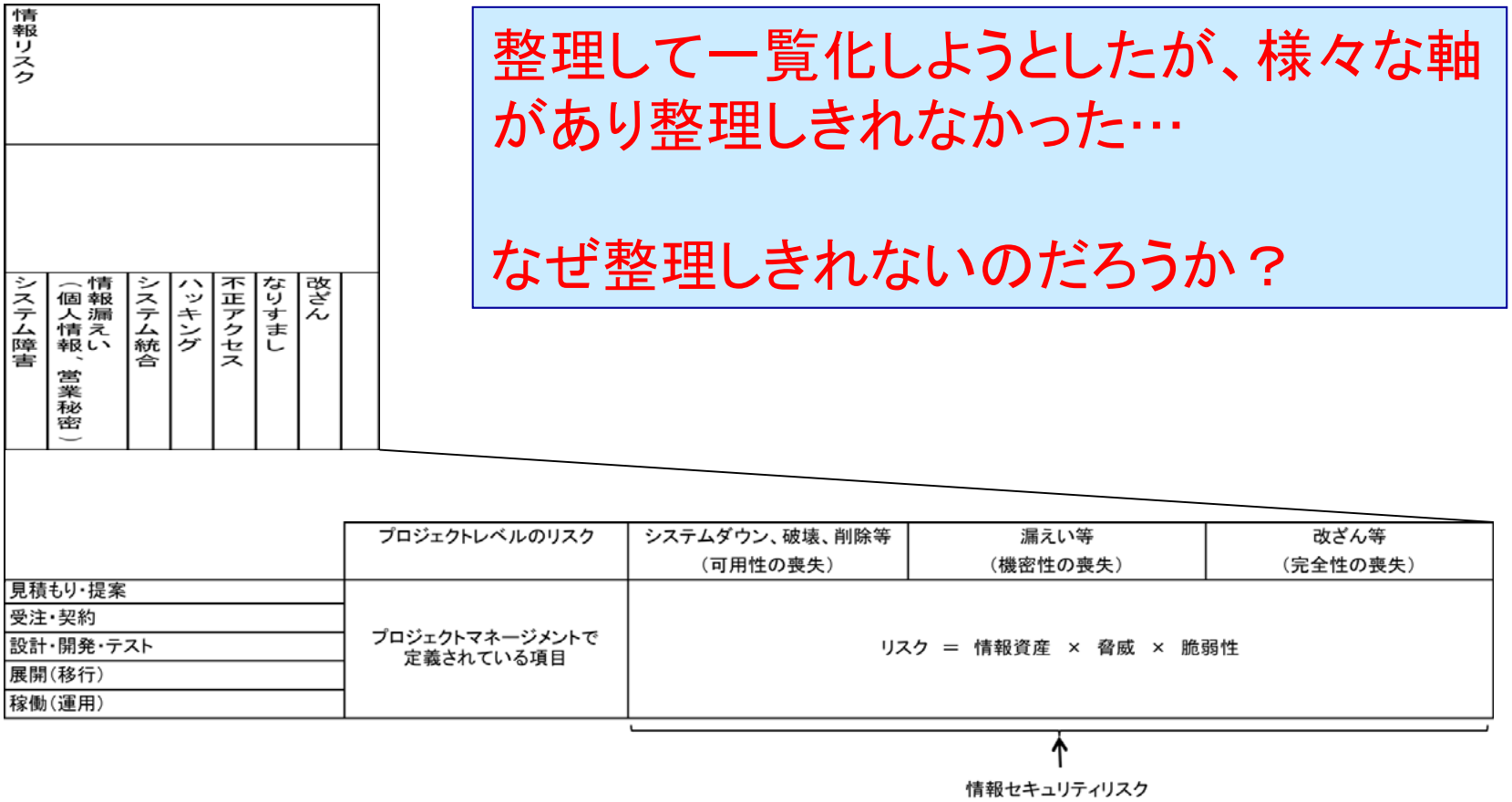
◆リスクを一覧化



分科会メンバが考えるリスク洗い出し、一覧としてまとめてみることにした。

リスクの洗い出し

◆リスクを一覧化



整理して一覧化しようとしたが、様々な軸があり整理しきれなかった…

なぜ整理しきれないのだろうか？

リスクの洗い出し

◆振り返り～こんなやり取りがあった

私の仕事では、自然災害や法制度の改正、為替変動などの影響が大きい。

私は主にセキュリティや事業継続のリスクを管理する立場だ。

ITIL®でいうと、変更管理、ITサービス継続性管理などがリスク管理に該当する。

ビジネスチャンスも好機のリスクである。プラスのリスクも考慮するべきだ。

リスクの洗い出し

◆振り返り～こんなやり取りがあった

みんな色々なこと言っているけど・・・

それって全部リスクだよね！！！

リスクの洗い出し

◆振り返りまとめ

✓リスクは、業務内容や立場により様々。

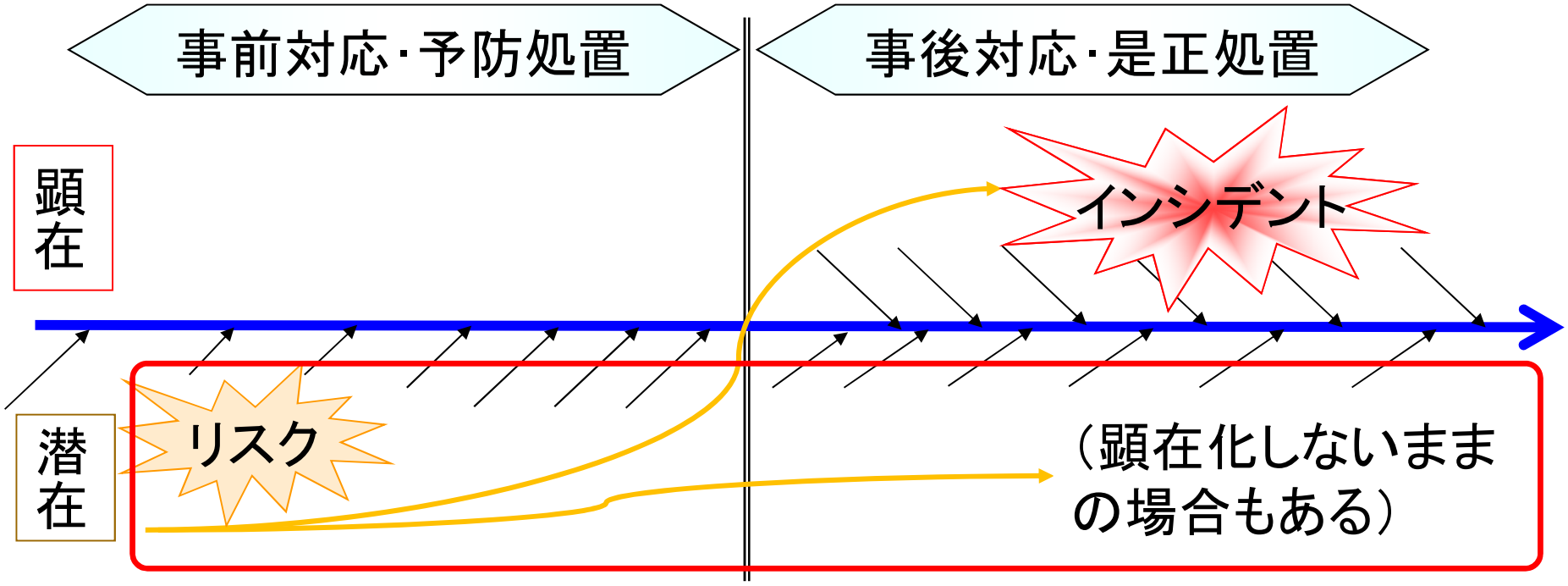
✓リスクには脅威だけでなく、中立や好機のリスクも存在。

✓災害・事故・政治・経済・社会・経営・情報・プロジェクトなど多岐にわたる。

各人が考えるリスクは様々だったが、ひとつひとつは全員が納得できるものだった。リスクは、立場や職務によって捉え方が異なるため、リスクの定義がメンバ全員で思いが違っていたことが、一覧化を難しくしていた。
そこで、リスクとは何か考えてみることにした。

リスクとは何か？

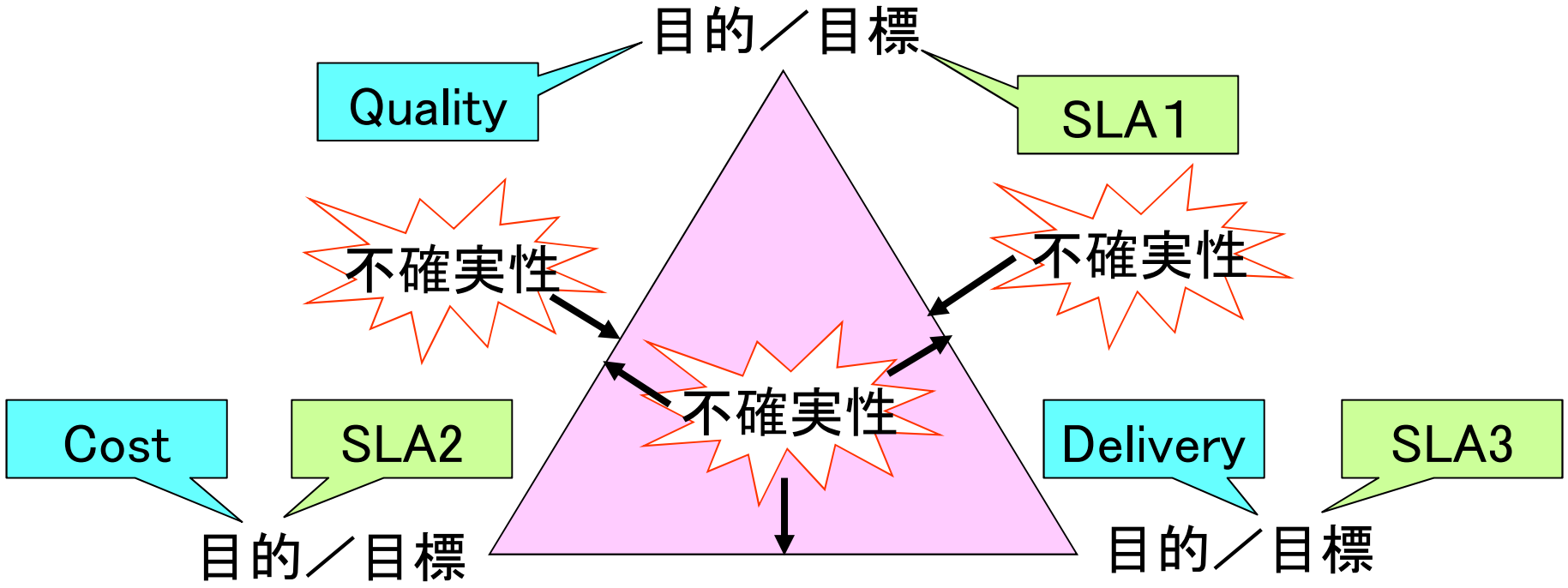
◆リスクは、問題・既知エラーとは異なる



顕在化していない、目的を阻害する外部要因／内部要因を研究対象とした。（顕在化したらイベント・インシデント）

リスクとは何か？

◆リスクは、目的・目標に対する不確実性



リスクとは目的・目標に対する不確実性であり、目的・目標が変われば、それらに対する不確実性も変わる。

リスクマネジメントの課題

◆なぜリスクマネジメントに苦労するのか？

リスクとは何か、意識を合わせることができた。
しかし実際の職場では、意識をあわせるだけでは、リスク洗い出しも含めたリスクマネジメントの活動がスムーズに実施できない状況にあるとの意見もでてきた。

なぜ苦労するのか？リスクマネジメント課題についてどのような内容があるのか考えてみた。

リスクマネジメントの課題

◆課題として考えられることを抽出

No	内容	活動分類	原因分類 人材	組織	費用	時間
1	リスクを認識していない。	洗い出し	●			
2	リスクに気が付いていない。	洗い出し	●			
3	忙しく、リスクアセスメントの時間がない。	洗い出し				●
4	リスクを認めようとしない。	洗い出し		●		
5	費用がかかる。予算化していない。	洗い出し			●	
6	リスクは自分の責任と思い込んでいる上司がいる。	洗い出し		●		
7	上司が理解してくれない。	洗い出し		●		
8	リスクを認識しても、自分には関係がないと切り捨てる。	コントロール	●			
9	他山の石。	コントロール		●		
10	自分だけは大丈夫、避けられると思ってしまう。	コントロール	●			
11	簡単に片づけたい。事を大きくしたくないと思う。	コントロール			●	
12	今すぐの課題ではないので、後回しにしている。	コントロール		●		
13	リスクを認識していない。その要因がリスクと思っていない。	洗い出し	●			
14	リスクを理解していない。表面のリスクのみで、本質を探っていない。	洗い出し	●			
15	本人がリスク。その人本人が阻害要因となってしまっている。	洗い出し	●			
16	そのリスクの影響度が判断出来ない(しない)。	コントロール		●		
17	リスクに対して過剰対応を行う。過剰反応してしまい、本質が見えなくなる。	コントロール		●		
18	臭い物に蓋。	洗い出し		●		
19	人員の不足。リスク管理を行うための人員を、規模や環境に応じて用意する必要があるが、そのための余剰人員や確保するのは企業側の理解がなければ難しい。	洗い出し				●
20	一般社員のリスクの理解度の不足。優れたリスクマネジメントの仕組みを整えたとしても、実践スベき一般社員がリスクの重要性自体を理解していない場合はリスクは管理できない。	洗い出し	●			
21	経営者・管理側のリスクの理解度の不足。管理側がリスクマネジメントを理解して以内場合は、リスク対策自体が取られない場合もある。	コントロール	●			
22	経営者・管理側のリスクの理解度の不足。リスク対策が必要と理解していても、その対策のために必要な情報や知識がなければ不十分な対策となる。	コントロール	●			
23	リスク管理を行うための予算不足。対策に回すための予算がない場合、十分な対策が取られないことが多い。	コントロール			●	
24	リスク管理を行うための予算不足。ただし、予算と天秤にかけてリスクの保有を選択した場合を除く。	コントロール			●	
25	リスク対策に割く時間の不足。リスク対策を行うための時間の不足。人員の不足とほぼ同じ。	コントロール				●
26	リスク対策に割く時間の不足。リスクの発生から対応までの、純粋な意味での時間の不足。	コントロール				●
27	環境の要因。実行する企業側に権限がない(オーナー、株主、親会社等)。	コントロール		●		
28	環境の要因。所在地に起因する要因(天災、カントリーリスク等)。	コントロール	●			
29	組織(役割・権限・責任)での立場により、リスクに対し理解・認識の温度差がある。経営トップのリスクマネジメントの重要性に対する認識・明確な方針の甘さ。また、社員への浸透性の甘さなど。(組織立ってコントロールされていない)	コントロール		●		

内容	活動分類	原因分類 人材	組織	費用	時間
、それ相当のスキルをもった人材がいない。	コントロール	●			
化などの風土が整っていない。	コントロール		●		
らいため、もの(新技術・設備などの環境)へのコスト投資(負担)がで	コントロール			●	
PDCA)するための時間が取れない。(重要な業務の1つとして捉えて	コントロール				●
、起きるかもしれないの裏返し「たぶん起きないだろう」という意識。	洗い出し	●			
	コントロール	●			
なければならない。(コストをかける余裕がない)	コントロール			●	
響)が想像できない。	コントロール	●			
像できない。	洗い出し	●			
	コントロール		●		
状況により組織全体に浸透せず、結果リスクマネジメントが進まな	コントロール		●		
、リスクをリスクとして認識できないため、必然的にリスクマネジメント	洗い出し	●			
性を説明できず、費用対効果を適正に表現できないまま、後回しに	コントロール			●	
気。エスカレーション体制が整備されていないため、誰に言えばよいの	洗い出し		●		
で・・・					
メントを実施するため、リスクが何かを選別できない。	洗い出し		●		
メントを実施している。	洗い出し	●			
保していない。(コントロール部分が中心となり、アセスメントを軽視し	洗い出し				●
、対策案が揃った時点で合意形成しようとするため、後からリスクの	洗い出し		●		
など)の基準が存在しない。	コントロール		●		
の視点しか保持していない。全体最適の視点が欠落している。	洗い出し		●		
ない。全体最適の視点が欠落している。	洗い出し	●			
いたリスクには関知しない。	洗い出し		●		
を実施しているため、リスクマネジメントと聞くと「またか…」とネガティ	コントロール	●			
53 リスクを挙げると対策を求められるため、リスクを提示したがらない。	洗い出し		●		
洗い出し	25	11	10	1	3
コントロール	28	9	10	6	3

どのようなリスクマネジメントの課題があるか、分科会メンバの経験等より53種類の課題を抽出した。

リスクマネジメントの課題

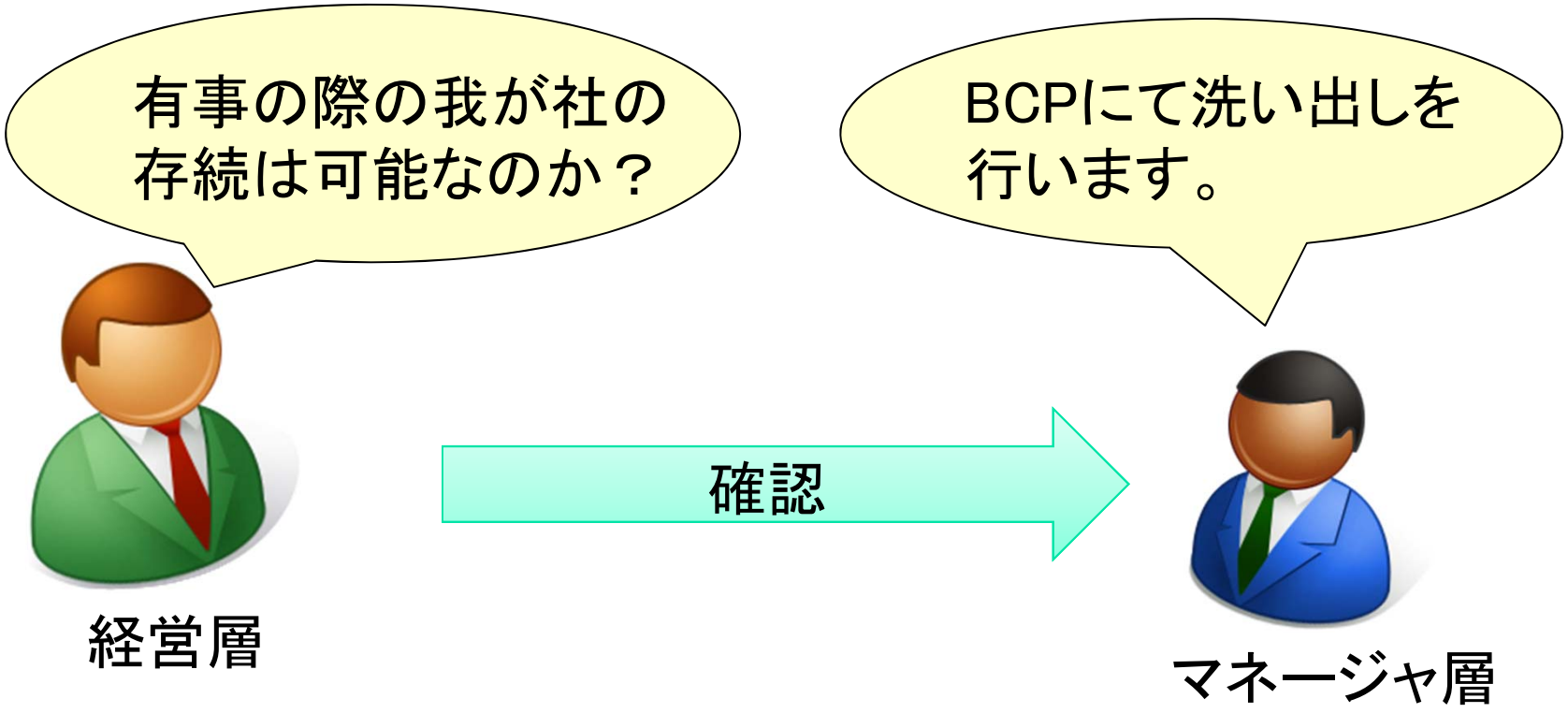
◆課題を分類

人材・組織に関する課題が多い

分類	説明	課題数	
		洗い出し	コントロール
人材	スキルセットや理解度、モチベーションに依存する課題	11	9
組織	活動範囲および権限、視点の違いに依存する課題	10	10
費用	活動に必要となる費用負担に依存する課題	1	6
時間	活動に必要となる工数に依存する課題	3	3

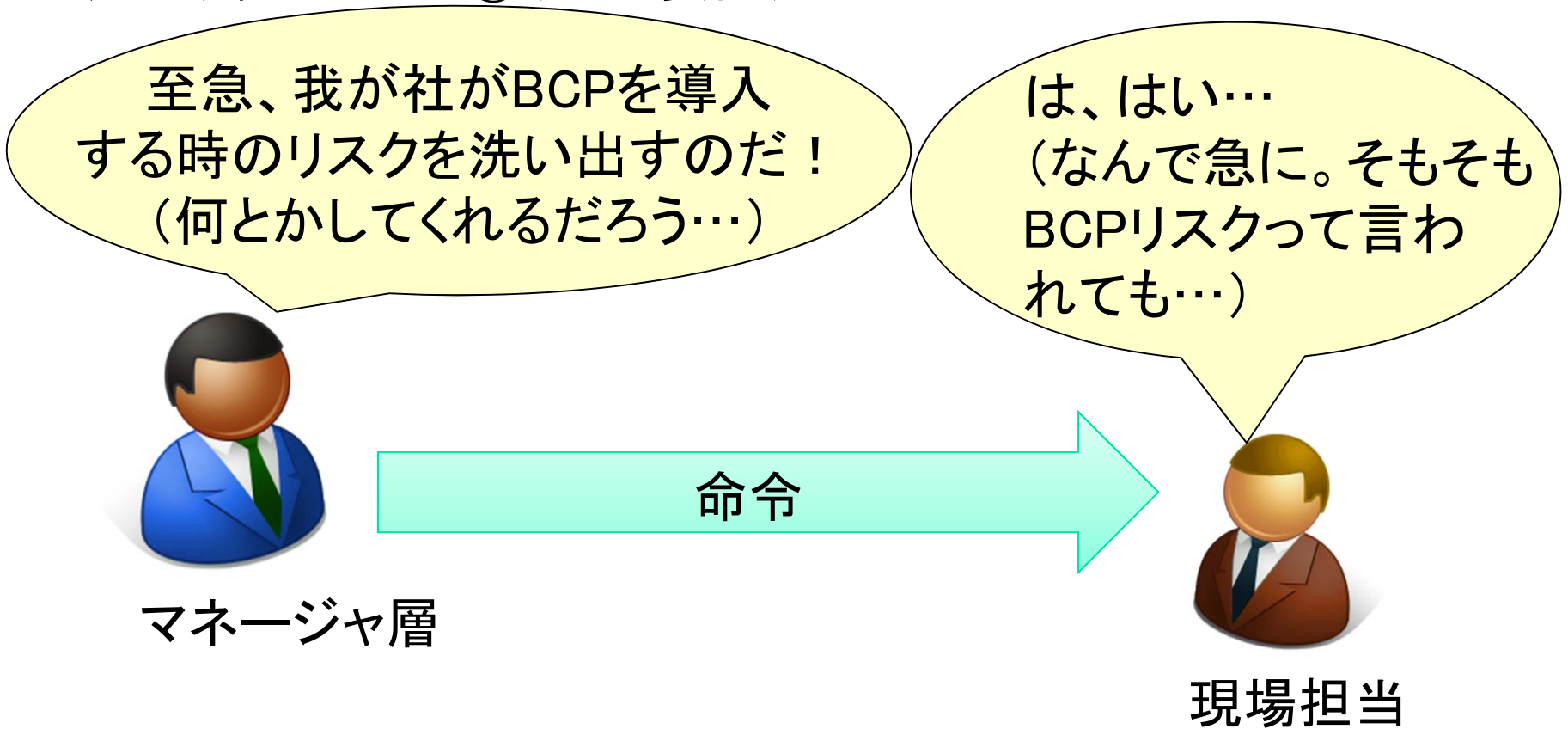
リスク洗い出しの阻害要因

◆起こりうるケース①（人的要因）



リスク洗い出しの阻害要因

◆起こりうるケース①（人的要因）



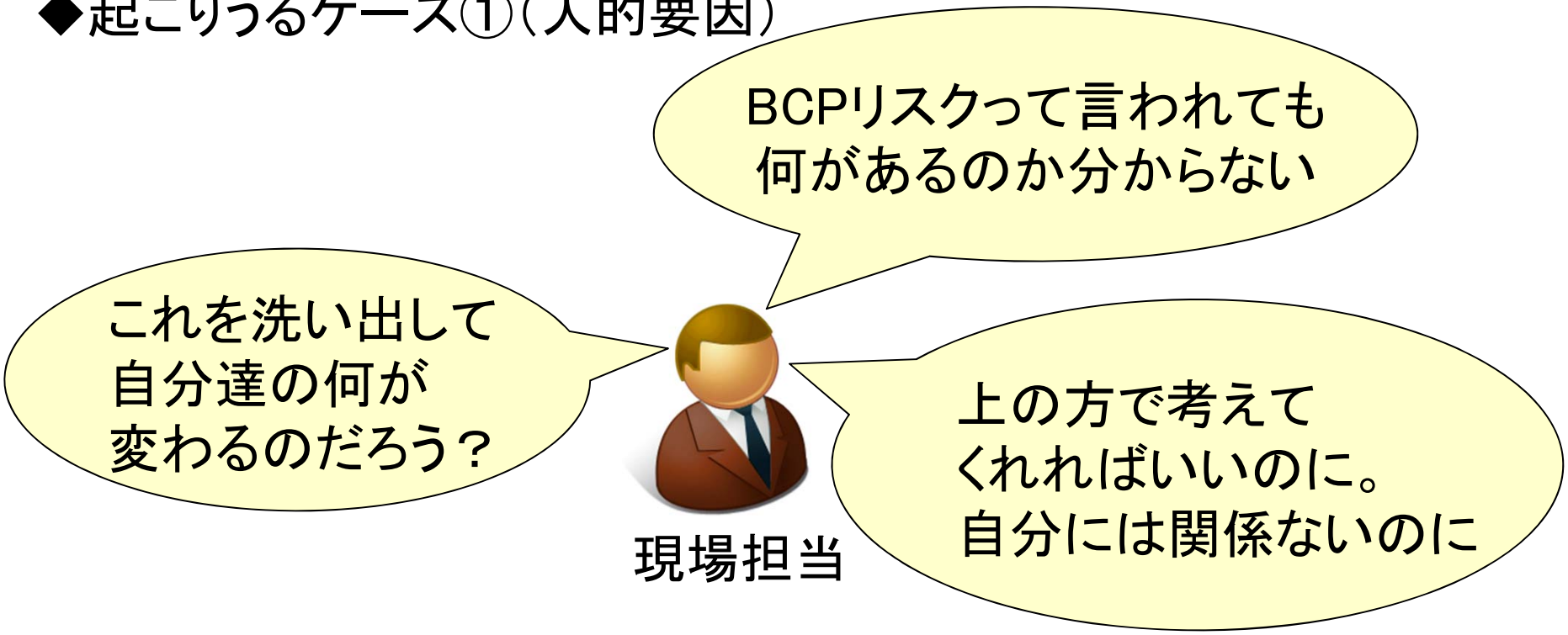
リスク洗い出しの阻害要因

◆起こりうるケース①（人的要因）

リスクについて考える余裕がない状態に陥り、現場の担当者へ任せきりにしてしまう。

リスク洗い出しの阻害要因

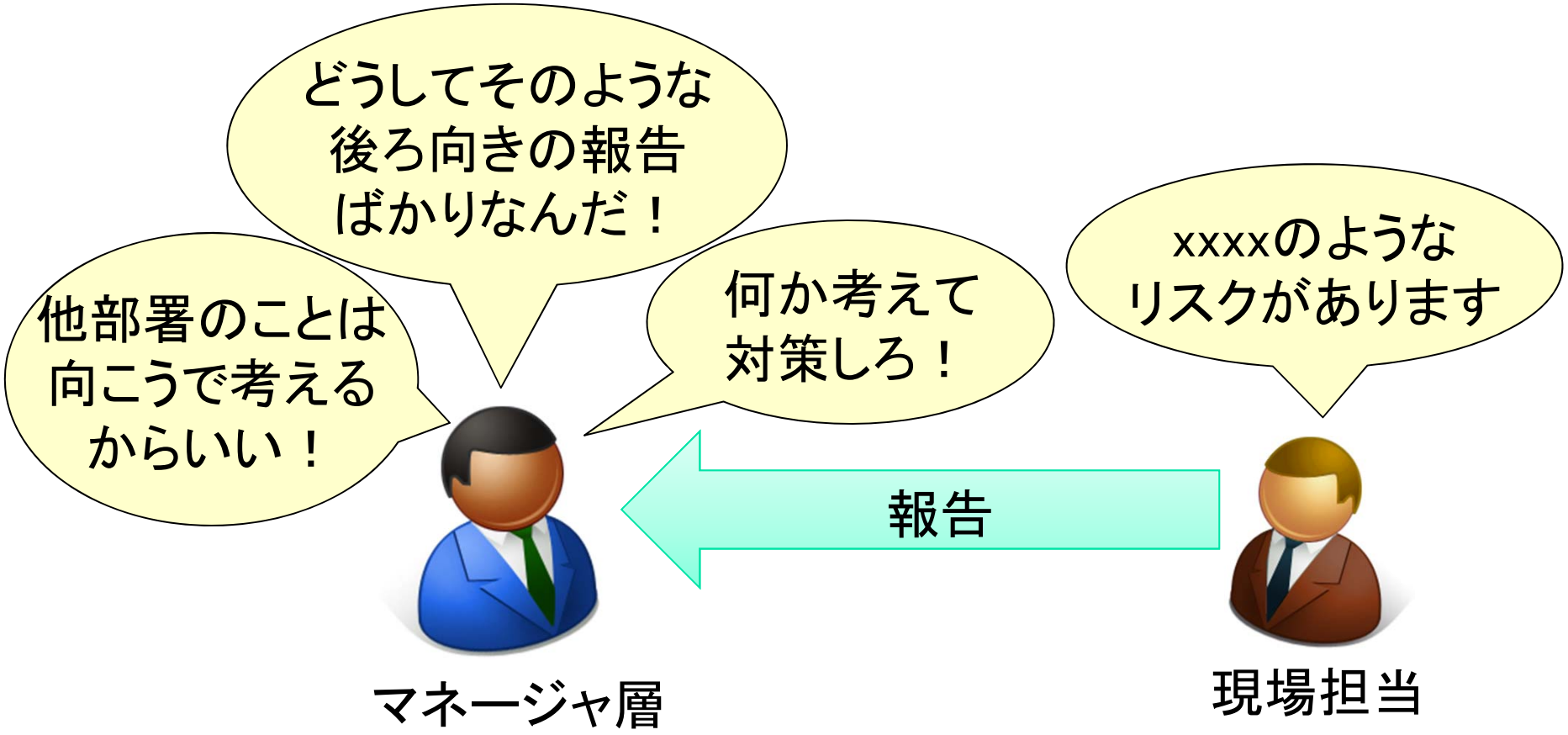
◆起こりうるケース①（人的要因）



必要性や目的の説明が不十分なのでやらされ感がある。
知識や経験不足により、洗い出しが不十分になる。

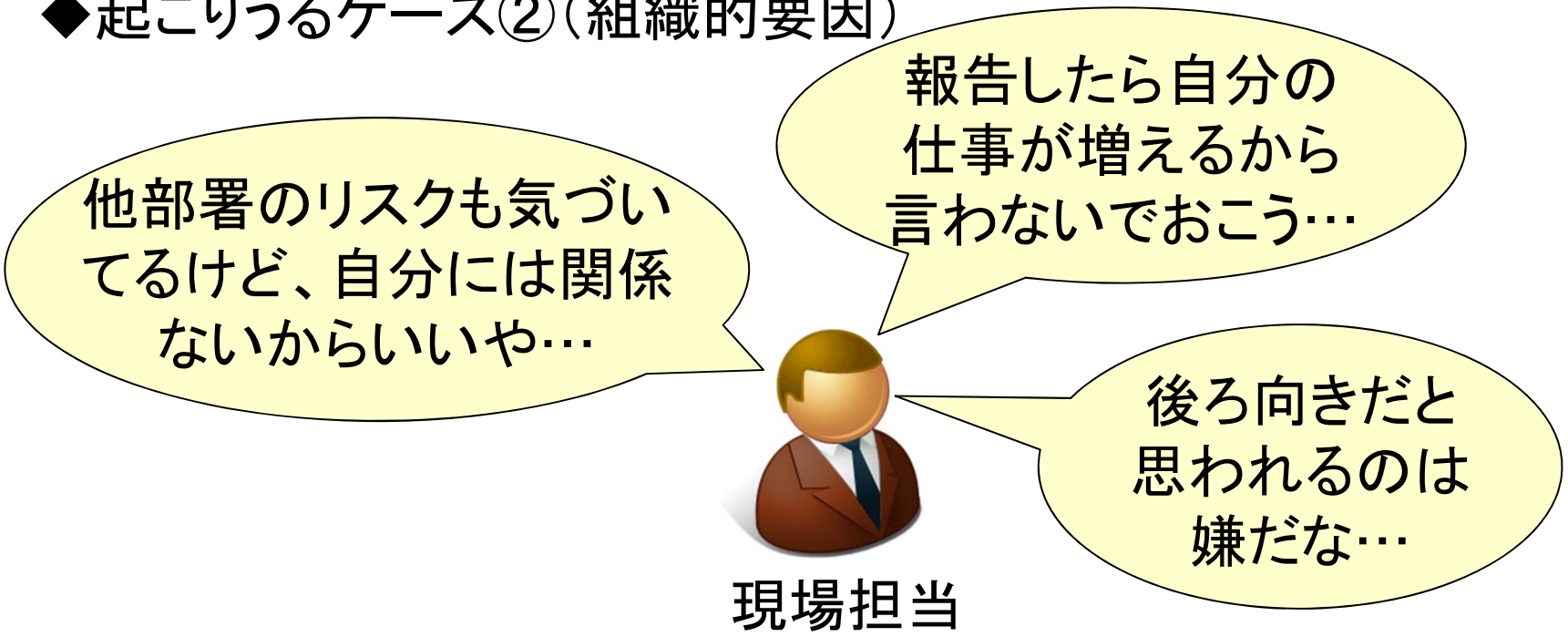
リスク洗い出しの阻害要因

◆起こりうるケース②（組織的要因）



リスク洗い出しの阻害要因

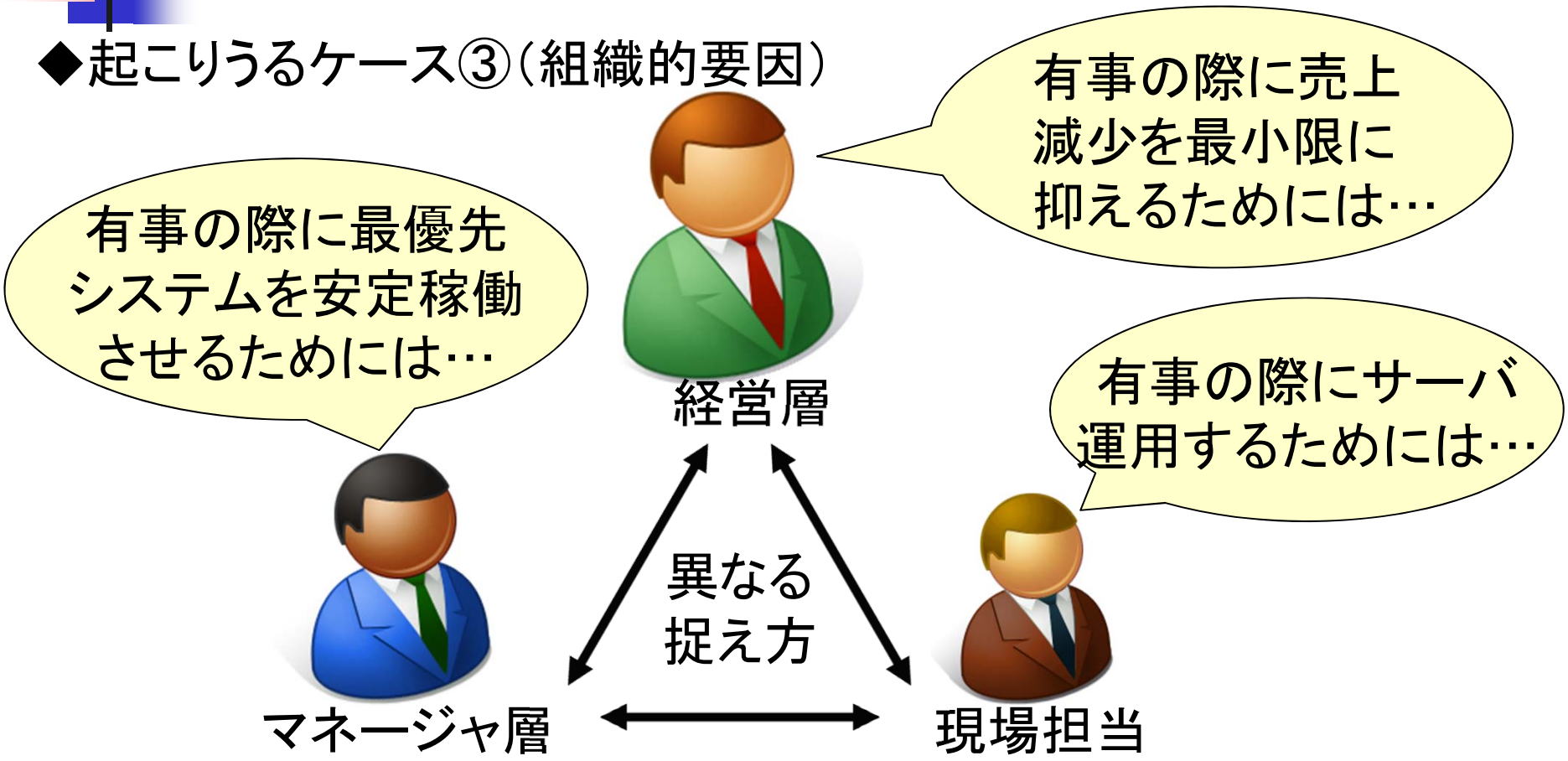
◆起こりうるケース②（組織的要因）



リスクに気がついていても、気がつかなかったことにしてしまう組織構造（組織文化）により、洗い出しが不十分となる。

リスク洗い出しの阻害要因

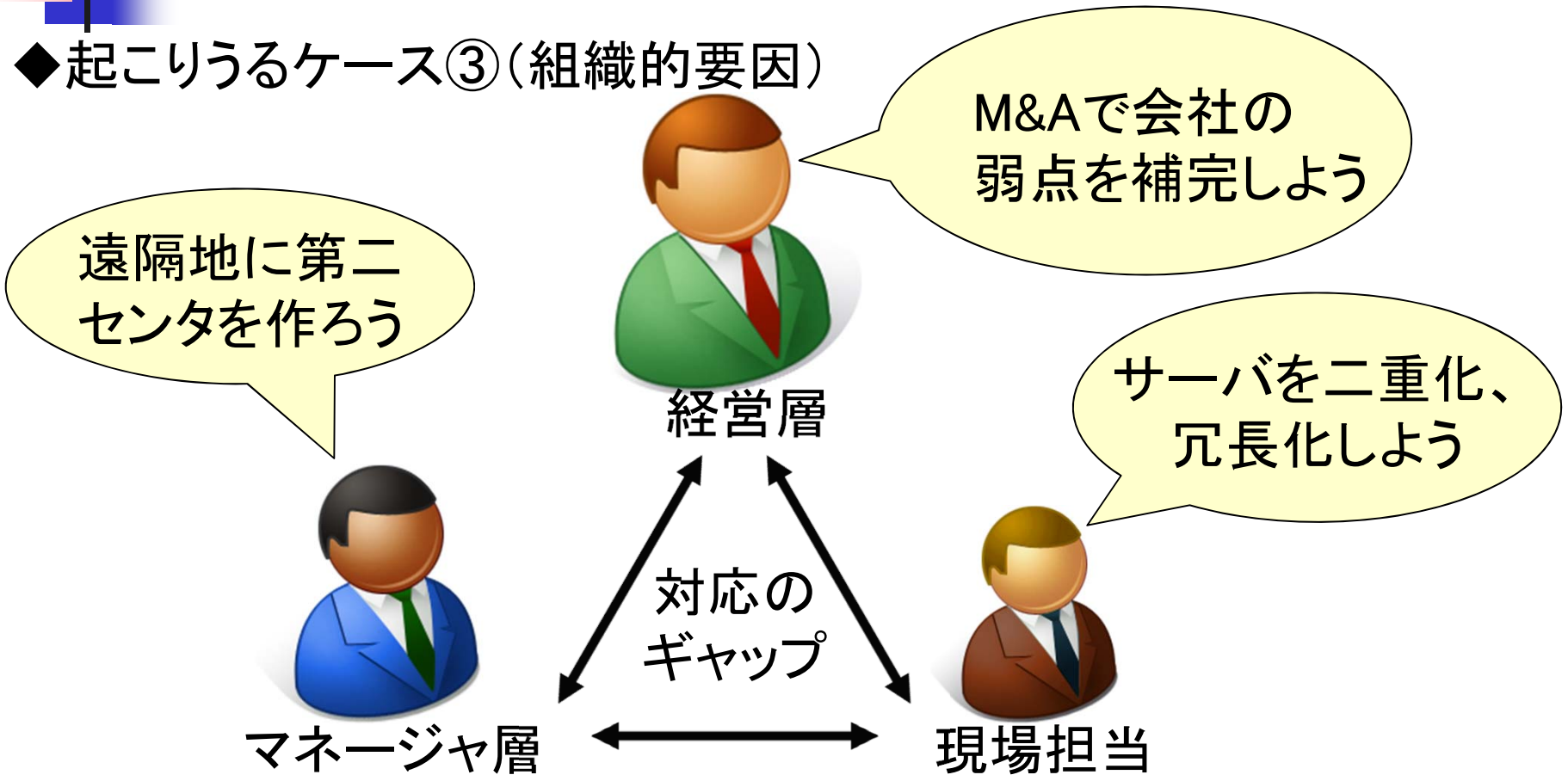
◆起こりうるケース③（組織的要因）



立場や職務による捉え方の違いに気づかずにいると・・・

リスク洗い出しの阻害要因

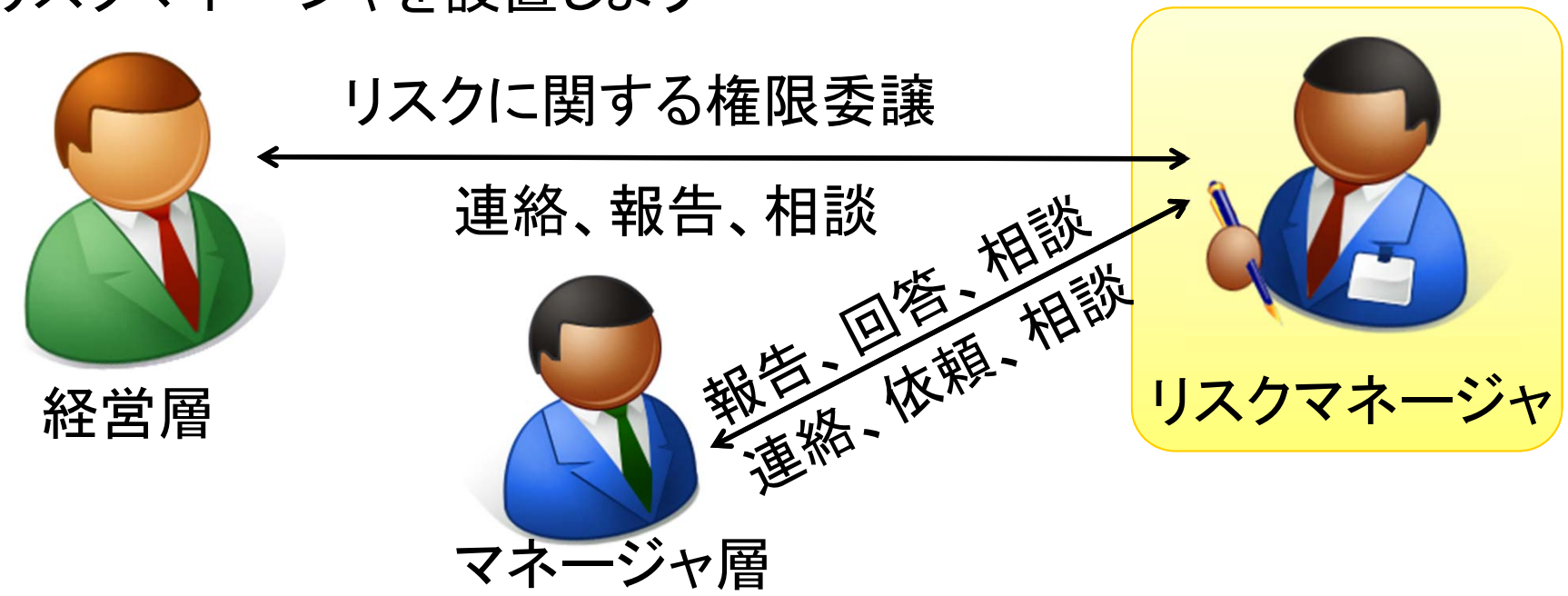
◆起こりうるケース③（組織的要因）



その後の対応が異なり、ギャップが発生してしまう。

阻害要因への解決策

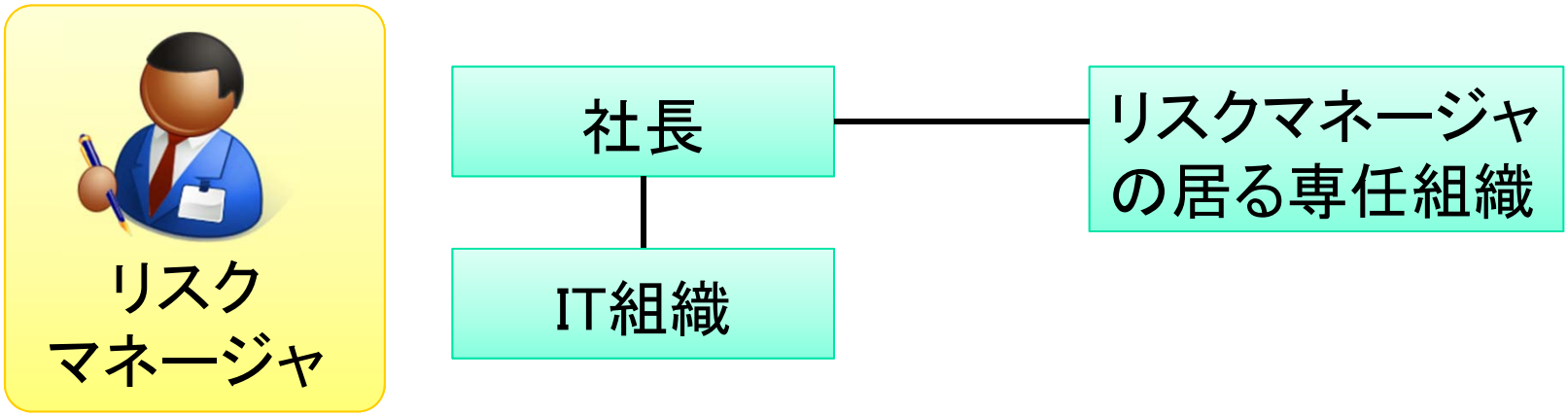
◆リスクマネージャを設置しよう



完全な専任組織としてリスクマネージャを設置し、経営層との直接の会話を行い、各マネージャへ協力体制を引いて、事案に対応する。

阻害要因への解決策

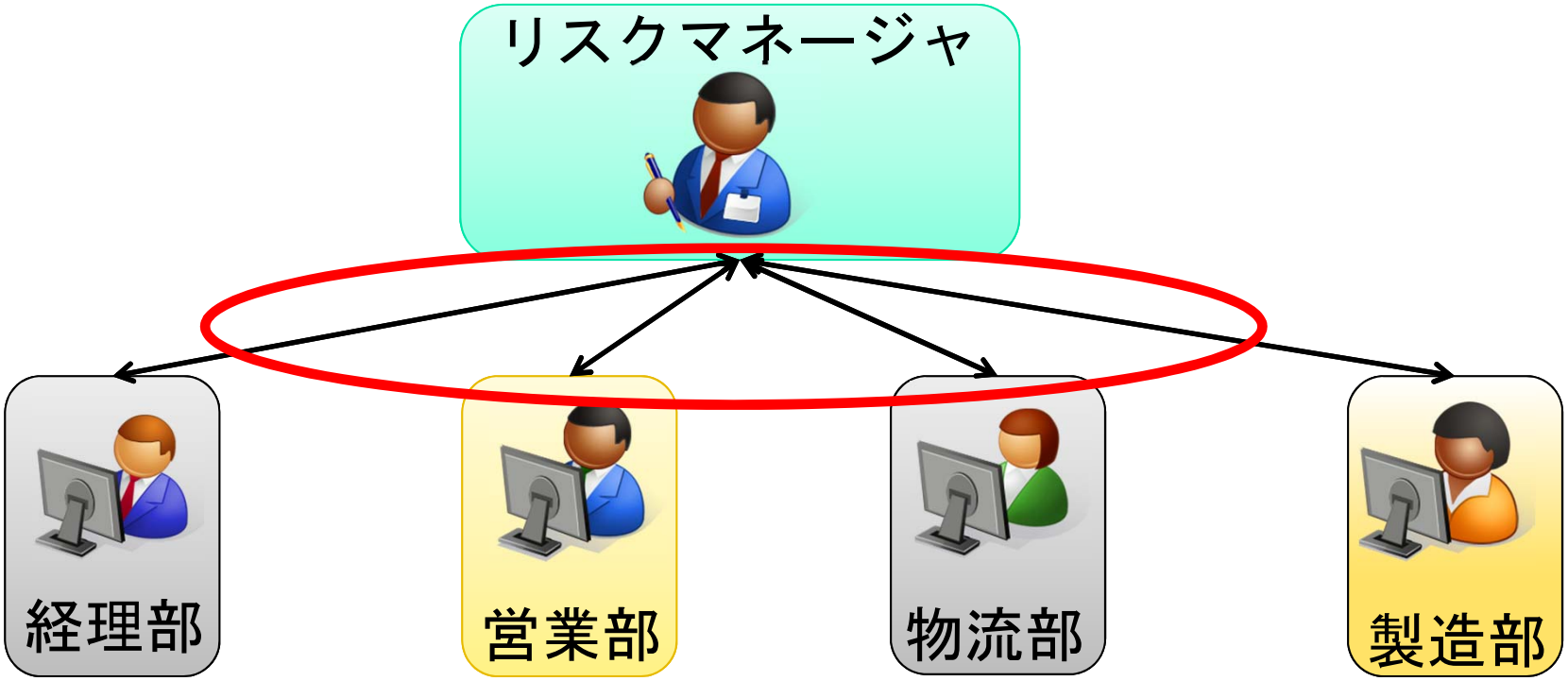
◆リスクマネージャの条件



・自社業務および業界を理解し、かつリスクに関する有識者。
　→知識、経験の不足を補完。
・リスクマネージャだけは専任とし、経営層の直轄とする。
（他の業務と兼務しない）
　→任せきりを排除し、中立性を保つ。

阻害要因への解決策

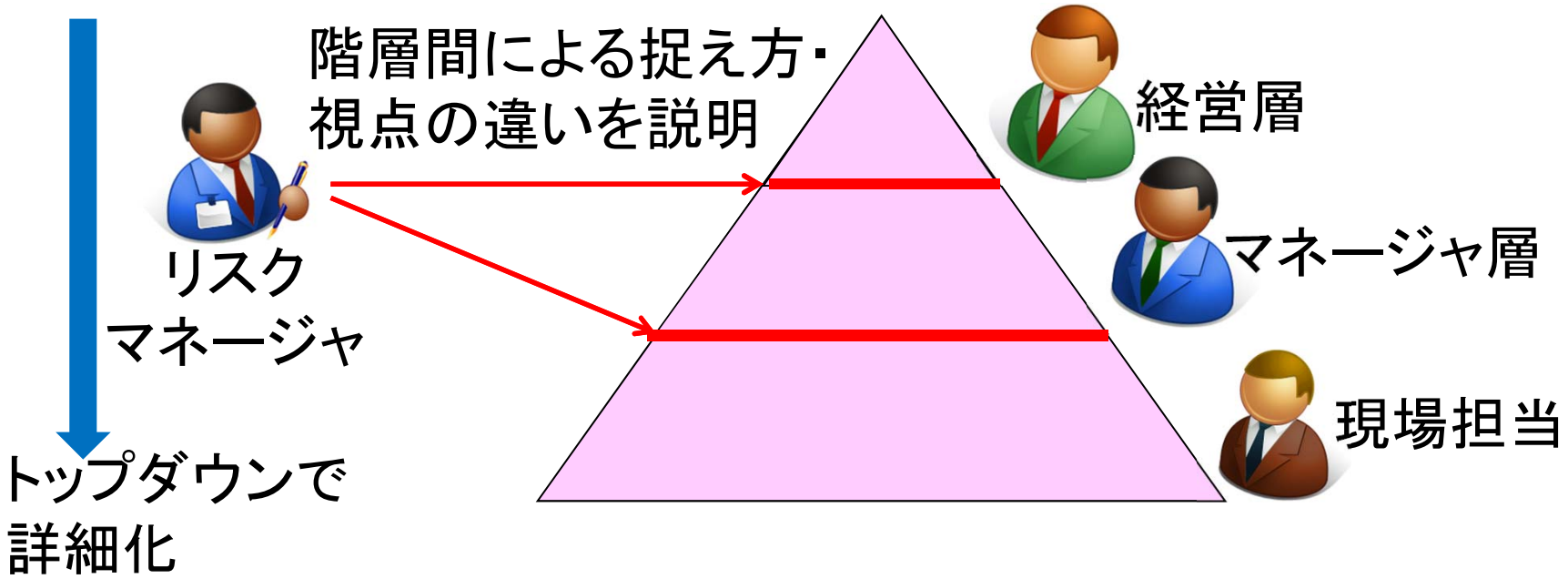
◆リスクマネージャの役割



捉え方の異なる、部門別で洗い出していたリスクを持ち寄って整理。リスクマネージャは、それをファシリテートする。

阻害要因への解決策

◆リスクマネージャの役割



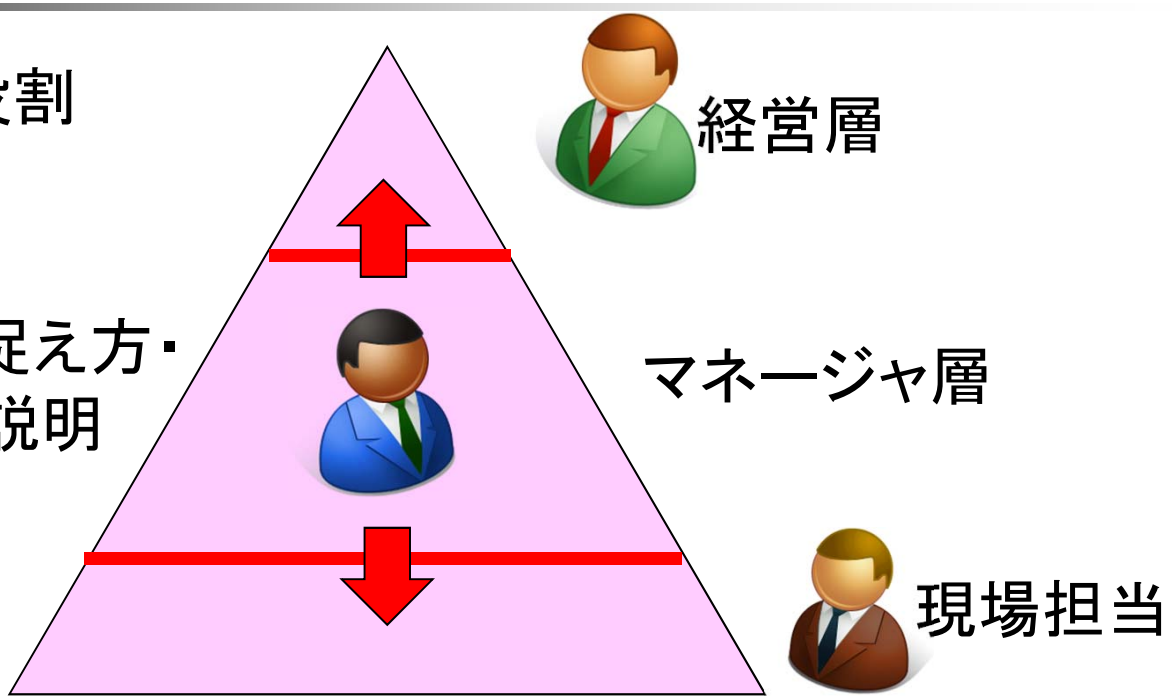
階層間で異なるリスクの捉え方の違いを説明する。
また、トップダウンでリスクを洗い出していくことにより、事業との整合性を保つことも可能となる。

阻害要因への解決策

◆マネージャ層の役割

階層間による捉え方・
視点の違いを説明

トップダウンで
詳細化



上位層の視点をマネージャ層が視点を変えて説明することにより、担当者は難しく考えずとも、普段からリスクの洗い出しを日常業務として行えるようにする。

まとめ

◆リスク洗い出しに必要なこと

Point リスクは、立場や職務によって捉え方が異なることを認識しよう！

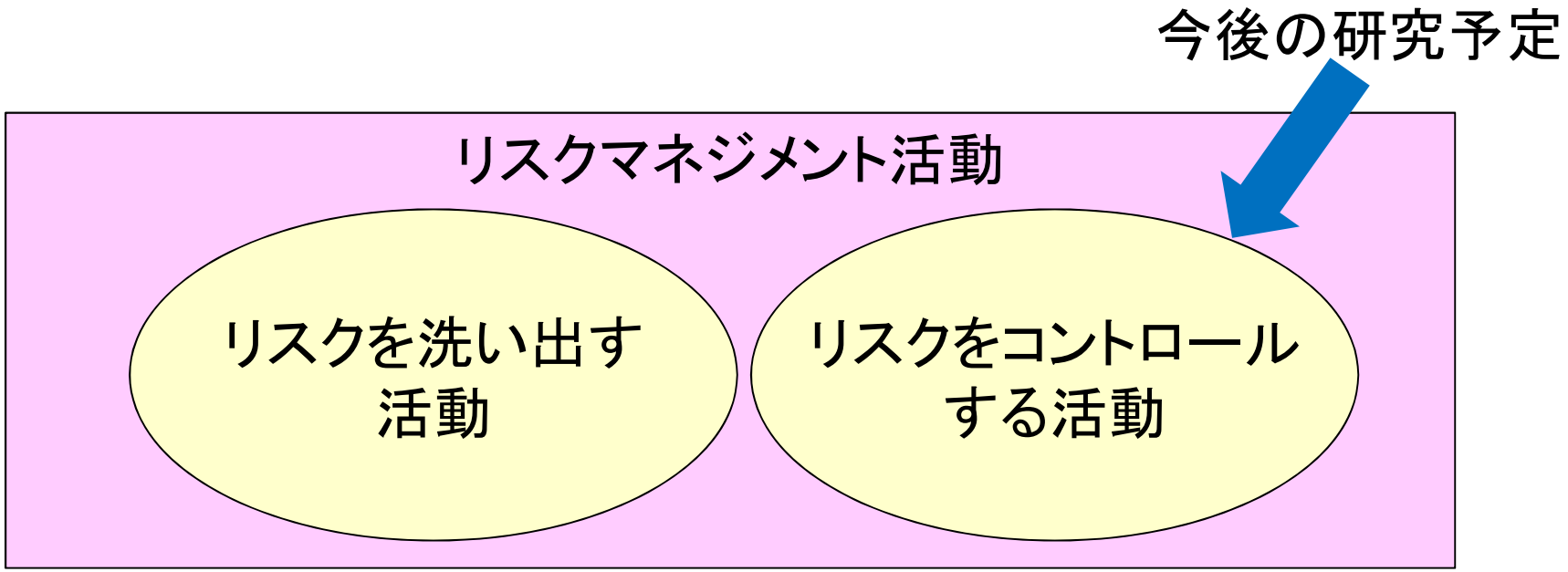
Point リスクの洗い出しを、現場の担当者へ任せきりにしないようにしよう！

Point リスク洗い出しの必要性や目的を、十分に説明しよう！

Point リスクを挙げやすい環境を整えよう！

リスクマネージャを設置し、リスクの洗い出しが容易になるような仕組みを作ろう！

今後の研究予定



洗い出したリスクに対し、どのようにコントロールしていくか、各フレームワークとの連携を含めて研究していく。

分科会紹介

◆リスクマネジメント研究分科会メンバ

- 座長　　：　白井祐司
- 副座長　：　江下善行、谷芳文
- メンバ：　阿部正峰、萱原渉、金田一啓史
  小林知美、角一己、寺島義人
  中谷英雄、松田浩幸、三浦康弘
  村上憲也、梁島泰之、山内裕史

分科会紹介

◆リスクマネジメント研究分科会メンバ

ご清聴
ありがとうございました