

---

# オペレーショナル・リスク管理の基礎

# 目次

---

1. オペレーショナル・リスクとは
2. 組織・体制
3. リスク管理の基本フレームワーク
  - リスクの識別、評価、モニタリング、削減/コントロール
4. 内部監査による検証
5. 更なる高度化に向けての課題

# 1. オペレーショナル・リスクとは

---



## 定義

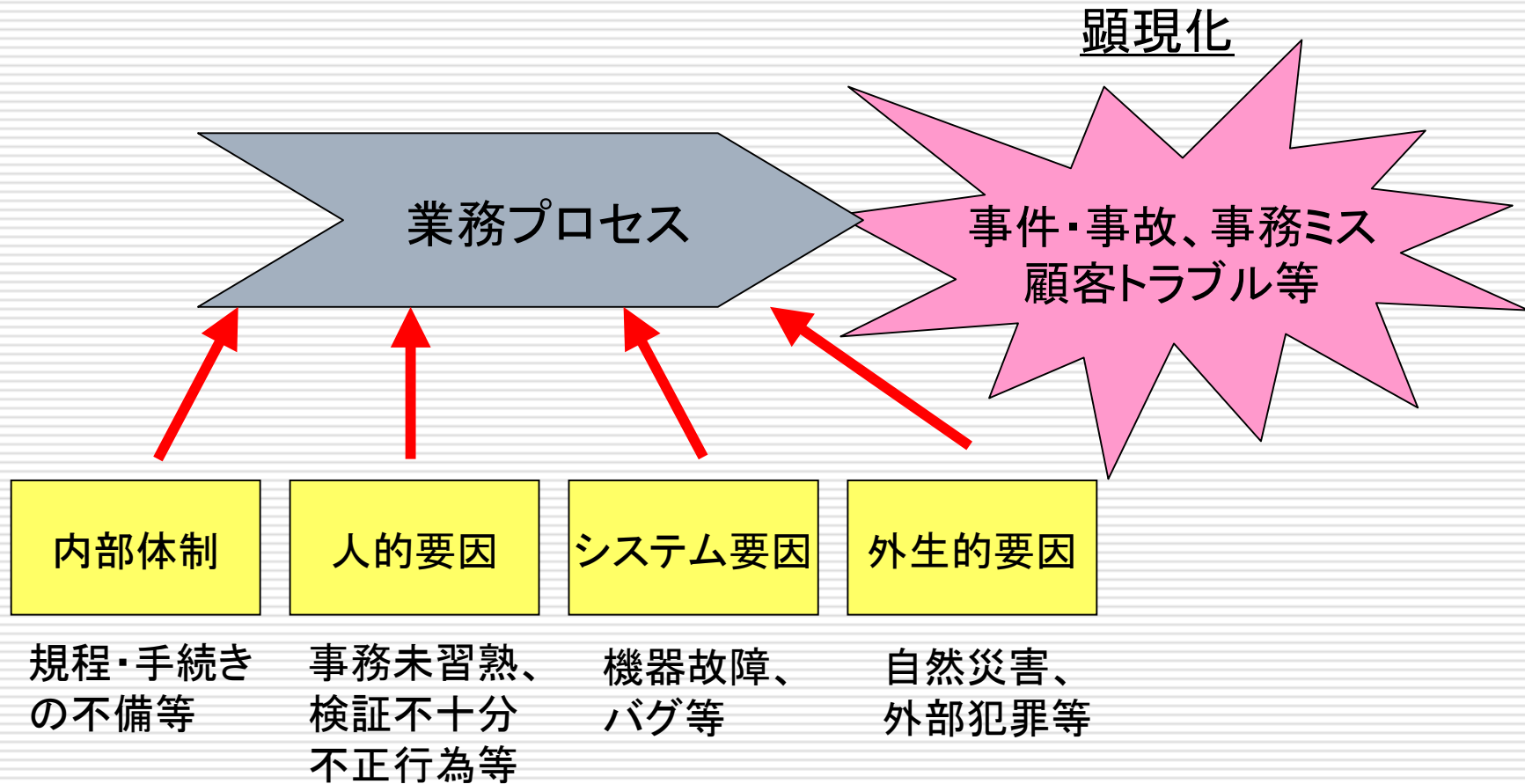
オペレーショナル・リスクとは、  
内部プロセス・人・システムが不適切であること  
もしくは機能しないこと  
または外生的事象が生起することから生じる損失  
に係るリスク

※バーゼル銀行監督委員会 2004年6月

「自己資本の測定と基準に関する国際的統一化:改訂された枠組」による定義。  
オペレーショナル・リスクは幅広い概念であり、管理対象は金融機関が自ら決める。

ただし、規制自己資本比率算定上のリスク計量化対象としては、法務リスクは含むが、戦略リスク、評判リスクは含まない。

# オペレーショナル・リスク(概念図)



# オペレーショナル・リスクの顕現化事例

---

## ■ 極めて多岐に亘る。

- 現金事故
- 現金、預金等の横領
- 重要用紙の紛失、不正流用
- 口座相違、為替誤送信
- 不正融資
- 保証付き融資の代弁否認
- 金融商品販売のコンプライアンス違反
- マネー・ロンダリング
- インサイダー取引
- システム障害
- 情報漏洩
- 市場運用の損失隠し
- 不正資産運用
- 不正会計処理
- 自然災害による被害
- テロ行為による被害
- 過労死
- ハラスメント
- 風評被害
- ⋮

## 2. 組織・体制

### － 全社的なリスク管理体制の構築

---

(オペレーショナル・リスクの特徴①)

- オペレーショナル・リスクは多種多様であり、組織内のあらゆる部署で発生する可能性がある。



(オペレーショナル・リスク管理のポイント①)

- 多種多様なオペレーショナル・リスクを、いくつかのカテゴリーに分類し、それぞれの管理部署を設ける。
- オペレーショナル・リスクの状況を一元的に把握・管理する統括管理部署を設け、全社的なリスク管理体制を構築する。

# オペレーショナル・リスクの分類

---

- 自らが管理しやすいようにオペレーショナル・リスクをいくつかのカテゴリーに分類する。

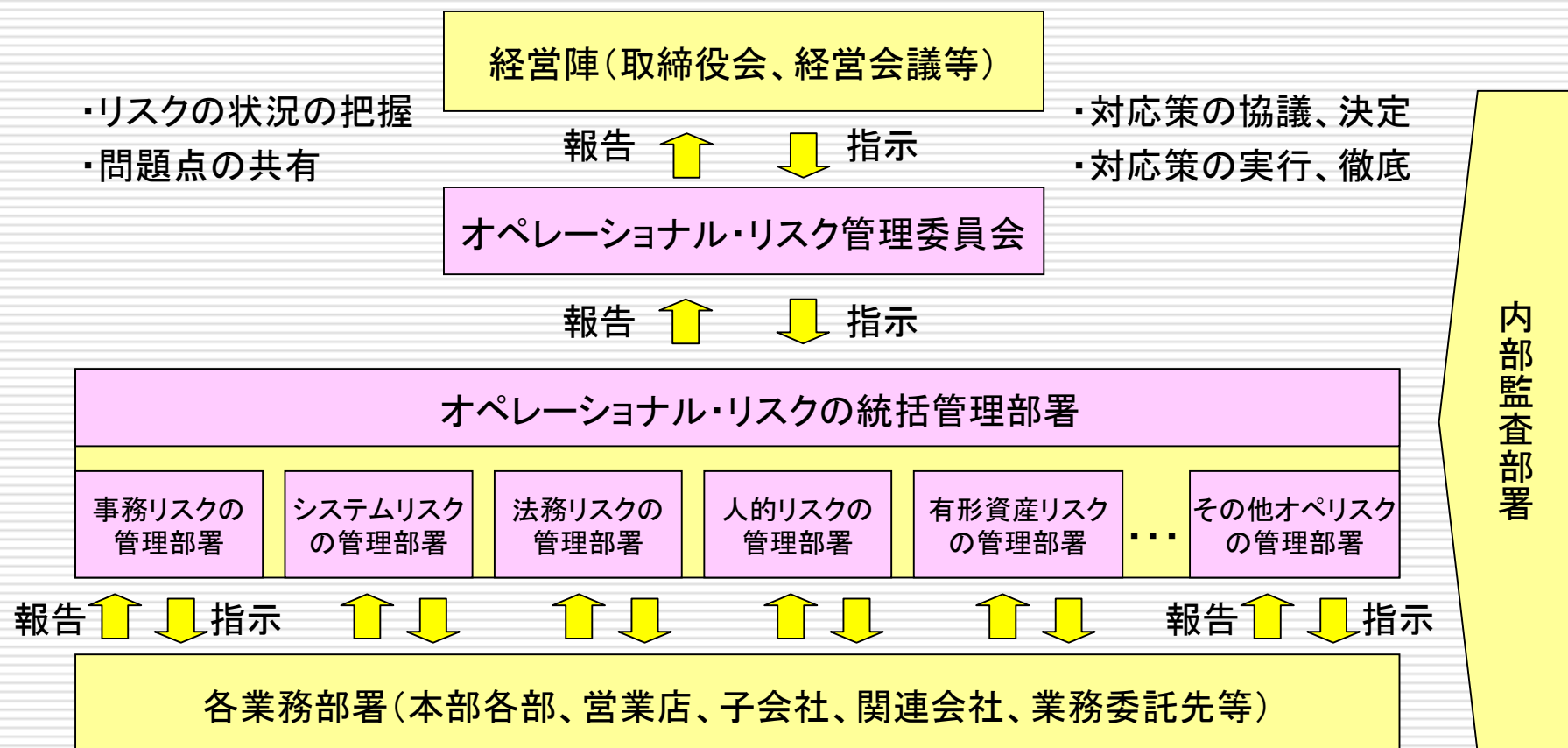


## 金融検査マニュアルによる分類の例示

- 事務リスク
- システムリスク
- その他オペレーショナル・リスク
  - ・法務リスク
  - ・人的リスク
  - ・有形資産リスク
  - ・風評リスク など※

※ 合理性があれば独自の分類でよい。金融機関によっては、上記のほか、情報セキュリティリスク、業務委託リスク等のカテゴリーを追加する先もみられる。

# オペレーショナル・リスク管理体制の構築(概念図)



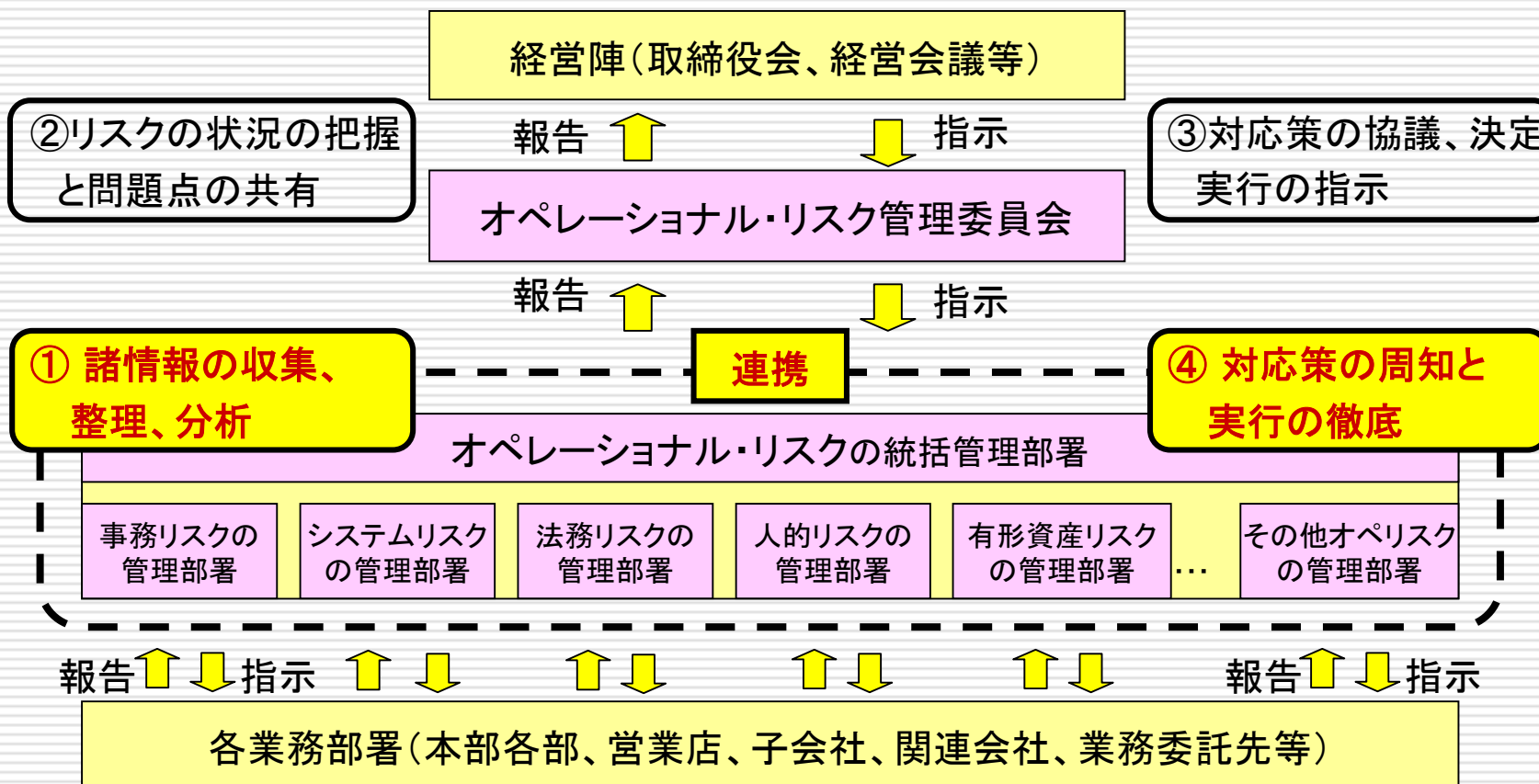


## リスク管理部署の連携による経営サポート

---

- 経営陣およびオペレーショナル・リスク管理委員会が、組織全体のリスクの状況を把握し、問題点を共有するためには、各種リスク事象に関する情報を収集、整理して、分析を行うことが重要。
- オペレーショナル・リスク管理委員会で協議のうえ、経営陣が決定した対応策については、組織全体に周知し、その実行の徹底を図ることが重要。
- したがって、オペレーショナル・リスク管理の実効をあげるためには、統括管理部署と各リスク管理部署が連携し、経営陣およびオペレーショナル・リスク管理委員会をサポートする体制を構築する必要がある。

# リスク管理部署の連携による経営サポート(概念図)



## リスク管理部署の連携による経営サポート

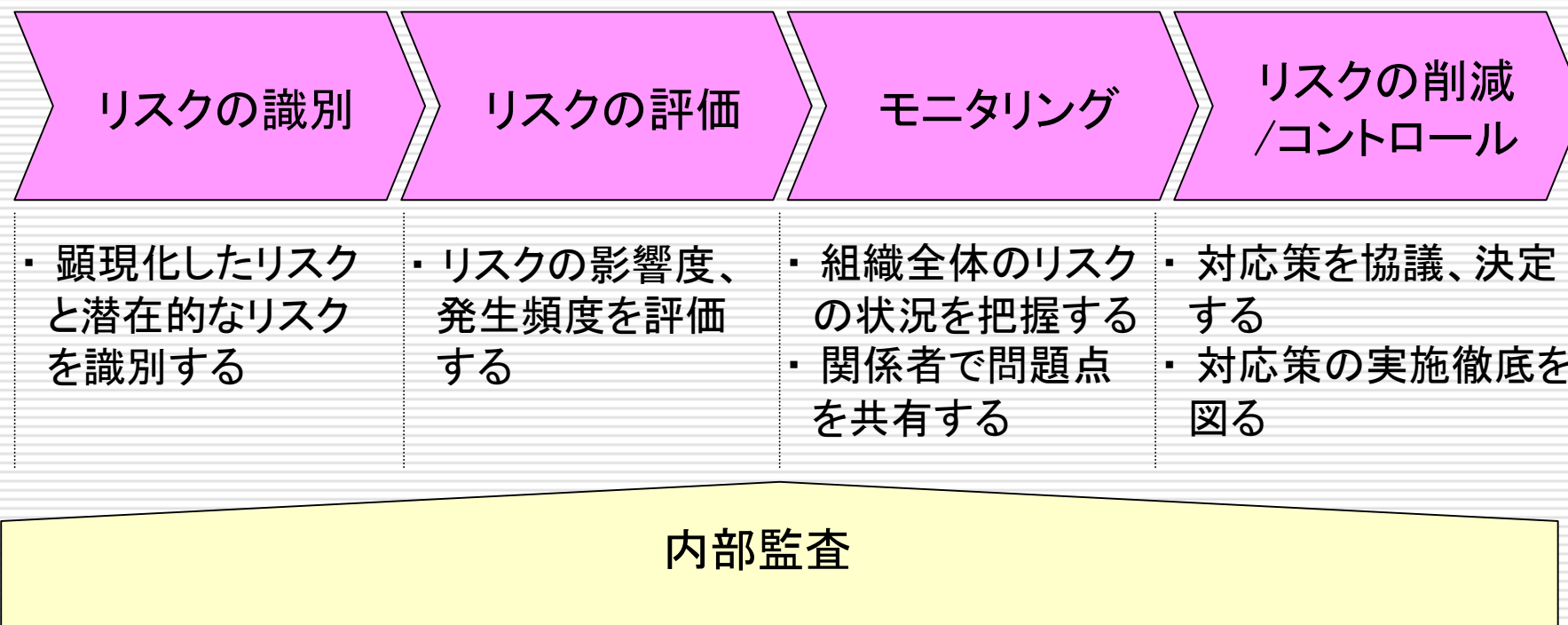
- オペレーショナル・リスクの管理では、実務に精通した担当者の組織横断的な連携によるチーム・サポートが不可欠。

(例)

- オペレーショナル・リスク管理委員会の下部委員会の設置  
各リスク管理部署、統括管理部署の実務担当者を下部委員会のメンバーとして配置。
- ワーキンググループ(WG)、タスクフォース(TF)の設置  
リスク事象のデータベース化、CSAの導入等にあたって、各リスク管理部署、統括管理部署の実務担当で組成したワーキング・グループ(WG)やタスク・フォース(TF)等をそのまま残存。
- 各リスク管理部署と統括管理部署の兼務体制  
各リスク管理部署の実務担当者を、統括管理部署に兼務要員として配置。

# 3. リスク管理の基本フレームワーク

バーゼル銀行監督委員会  
「オペレーショナル・リスクの管理と監督に関するサウンド・プラクティス」  
(2003/2)より



(参考)

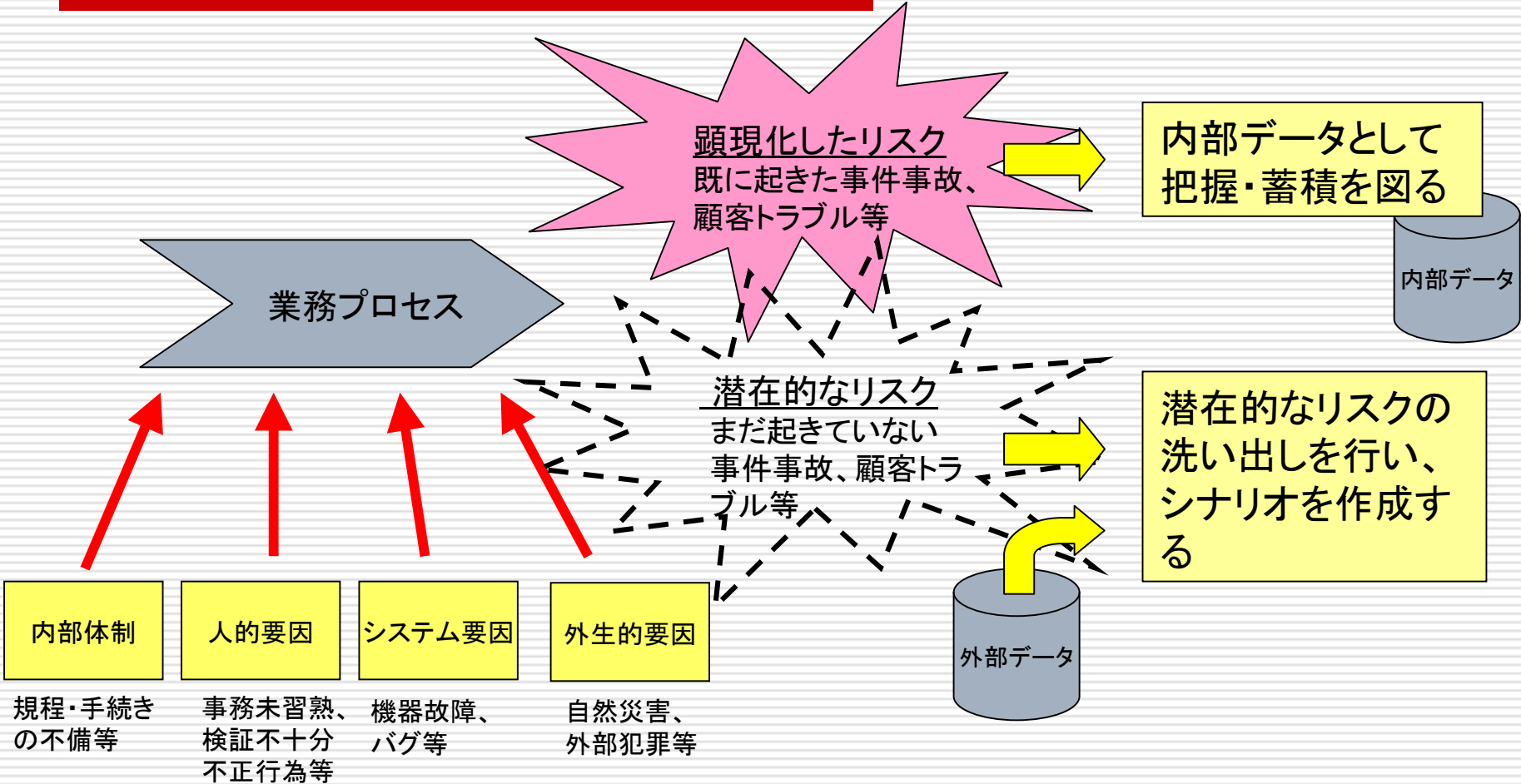


バーゼル銀行監督委員会

「オペレーショナル・リスクの管理と監督に関するサウンド・プラクティス」(2003/2)

銀行監督当局は、規模に拘わらず全ての銀行が、リスク管理の全体的な取り組みの一部として、重要なオペレーショナル・リスクの識別、評価、モニタリング、削減/コントロールのための効果的なフレームワークを導入することを求めるべきである

# 顕現化したリスクと潜在的なリスクの把握



## 顕現化したリスク事象のデータベース化

- 殆どの金融機関では、事件・事故、事務ミス、顧客トラブル等のリスク事象の発生に係る報告基準を定め、所管するリスク管理部署への報告を義務付けている。
- 近年、顕現化したリスク事象を分析するため、紙ベースの報告から電子ベースの報告に移行し、これらをデータベースに登録・蓄積する金融機関が増加している。
  - システム対応に関しては、自らデータベース・システムの開発を行う先、外部ベンダーのデータベース・システムを購入する先、スプレッド・シートで管理を行う先など、様々な形態がみられる。

## 顕現化したリスク事象のデータベース化

- リスク事象区分、データ登録項目は、リスク事象の分析目的や金融機関のリスクプロファイルにより異なる。
- データ登録・分析の目的、データ分析の有用性と登録負担を勘案して決定する。

(例) データ登録項目

リスク事象区分	独自区分(オペリスク・カテゴリーを更に細分化) and/or バンケル損失区分
発生日時	時刻、締め前後、曜日、五・十日、月末など
発生部署	部店、課、グループ、係、担当など
発生業務・プロセス	業務区分、プロセス区分、処理区分など
発生原因	発生原因が1つとは限らない。複数の原因がある場合もデータ登録を可能とする。
関係者情報	担当者、管理者、顧客などの属性情報
損失金額	直接費用 and/or 間接費用 and/or 機会費用



## 潜在的なリスクの洗い出し

---

- 潜在的なリスクについては、各業務に従事する者が洗い出しを行うのが有効。
- 各業務に従事する者がリスクの識別・評価を行う手法を総称して CSA (Control Self-Assessment) あるいは RCSA (Risk Control Self-Assessment) と呼ぶ。
- CSAには様々な手法がある。いずれの手法を採用する場合も「経営が重要と考えるリスク」を漏れなく、識別・評価することがポイント。



## 【事例①】潜在的なリスク事象の洗い出し手法

リスク事象を類型化し、それぞれの区分毎にリスクシナリオとして、どのようなことが想定されるか、各部署がリストアップする。

### リスク事象の類型化

カテゴリー	リスク事象区分
事務リスク	XXXX
	XXXX
	為替事故(誤送信・処理遅延等)
	XXXX
システムリスク	XXXX
	XXXX
	XXXX
法的リスク	XXXX
	XXXX
人的リスク	XXXX
有形資産リスク	XXXX
	XXXX
その他のオペリスク	XXXX
	XXXX

### (例)シナリオの作成方法

- ・リスク事象区分毎に  
○個のシナリオを作成
- ・一定金額以上の損失  
が発生するシナリオを  
列挙                    など

### シナリオの作成

**事務集中部**

シナリオ1  
担当者のオペミスを役席が看過。誤った口座に●億円を為替送金し、回収不能となる。

シナリオ2.  
繁忙日にオペ要員の配置が不足。為替の当日処理不能な案件が多数発生。損害賠償訴訟●億円を提起される。

シナリオ3  
XXXXXXXXXXXXXXXXXXXX

シナリオ4.  
XXXXXXXXXXXXXXXXXXXX

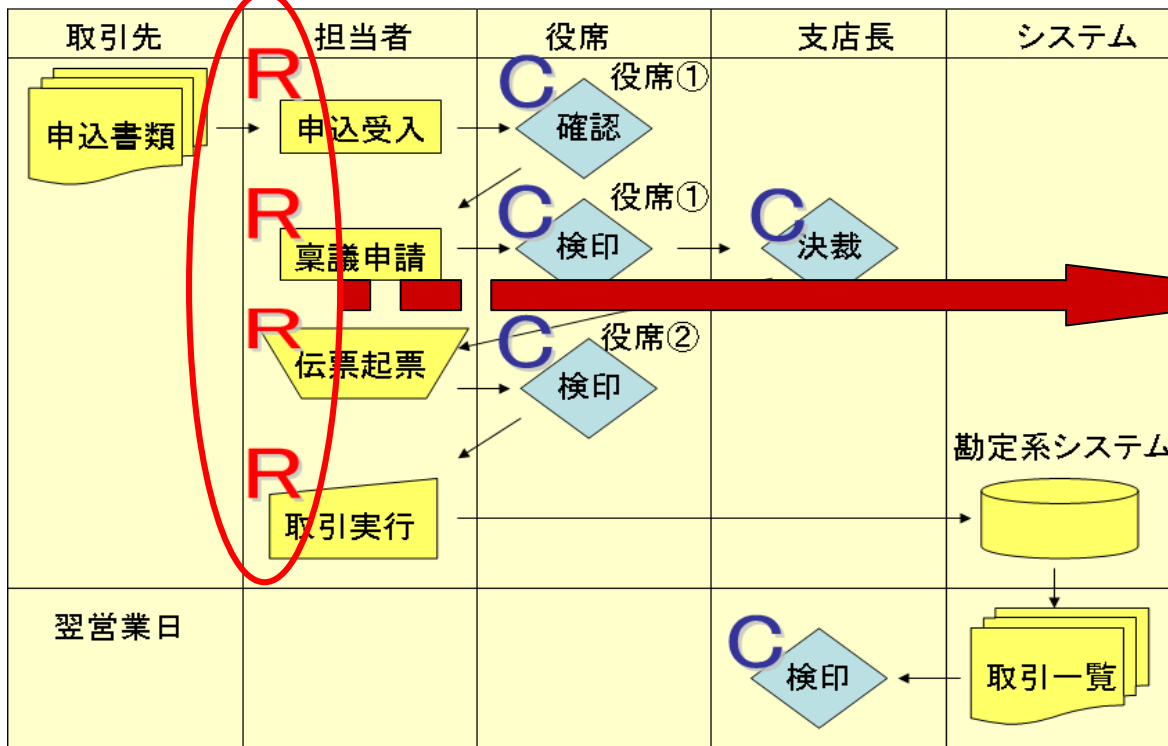
⋮

## 【事例②】潜在的なリスク事象の洗い出し手法

重要な業務プロセスを対象に、プロセスチャートを作成し、リスクの所在を確認しつつ、リスクシナリオを作成する。

### プロセスチャート

R : リスク C : コントロール



### シナリオの作成

#### 融資業務

##### シナリオ1

保証条件違反を看過し、保証協会付融資を実行。破綻後に、保証否認され●千万円の損失が発生。

##### シナリオ2.

融資実行を失念。顧客トラブルに発展。損害賠償訴訟●千万円を提起される。

##### シナリオ3

XXXXXXXXXXXXXXXXXX

##### シナリオ4.

XXXXXXXXXXXXXXXXXX

⋮

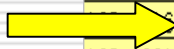
## (2) リスクの評価

- リスクの評価は「影響度」と「発生可能性」に基づいて行う。
- 残余リスクベースで評価するのが一般的。ただ、固有リスクやコントロールの有効性(統制リスク/脆弱性)に注目するケースもある。

リスク・コントロールマトリックス(RCM)

プロセス・コード	リスクの内容	リスク分類	固有リスクの評価		コントロールの内容	種類	評価	残余リスクの評価		優先度
			影響度	発生頻度				影響度	発生頻度	
123-001		事務ミス	大	大		予防的	有効	大	大	①
123-004		システム障害	中	中		発見的	概ね有効	中	中	②
		規程違反	小	小			不十分	小	小	③
123-021		内部不正					コントロール無			④
123-022		外部不正								⑤
123-067		自然災害								

内部データ



シナリオ



## 【参考】用語の定義

### 固有リスク

- ◆ コントロール等が全く整備されていないと仮定した場合に存在するリスク

### 残余リスク

- ◆ 不利な事象の影響と発生の可能性を軽減する措置(コントロール等)を講じた後にさらに残るリスク

### 統制リスク/脆弱性

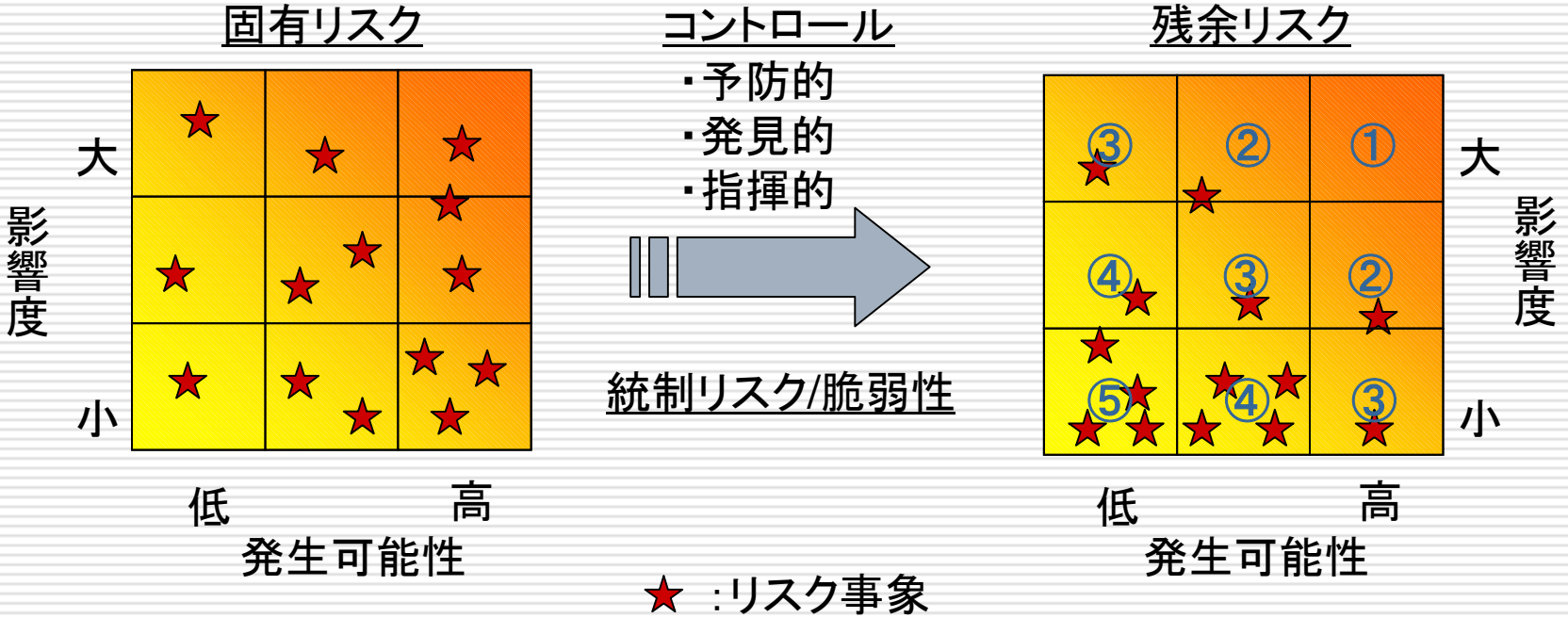
- ◆ 機能しないコントロール手続きに依存するリスク

統制リスク	小さい	大きい
脆弱性	低い	高い
コントロール	強い (有効である)	弱い (有効でない)

# リスク評価の様々な手法

## 事例① リスクマップ方式

- 残余リスクでみて、右上(左下)の方が重要度が高い(低い)。



## リスク評価の様々な手法

### 事例② リスク評点化方式

- 「影響度」、「発生可能性」、「コントロールの有効性」を評点化し、乗じることによって、残余リスクを評点化する。

(例)

リスク内容	固有リスク		コントロール	残余リスク
	影響度 (評点A)	発生可能性 (評点B)	有効性 (評点C)	評価 (評点A×B×C)
為替誤送信	○点	△点	◇点	○×△×◇点
預金横領	●点	▲点	◆点	●×▲×◆点
⋮	⋮	⋮	⋮	⋮



## リスク評価の様々な手法

### 事例③ リスク計量化方式

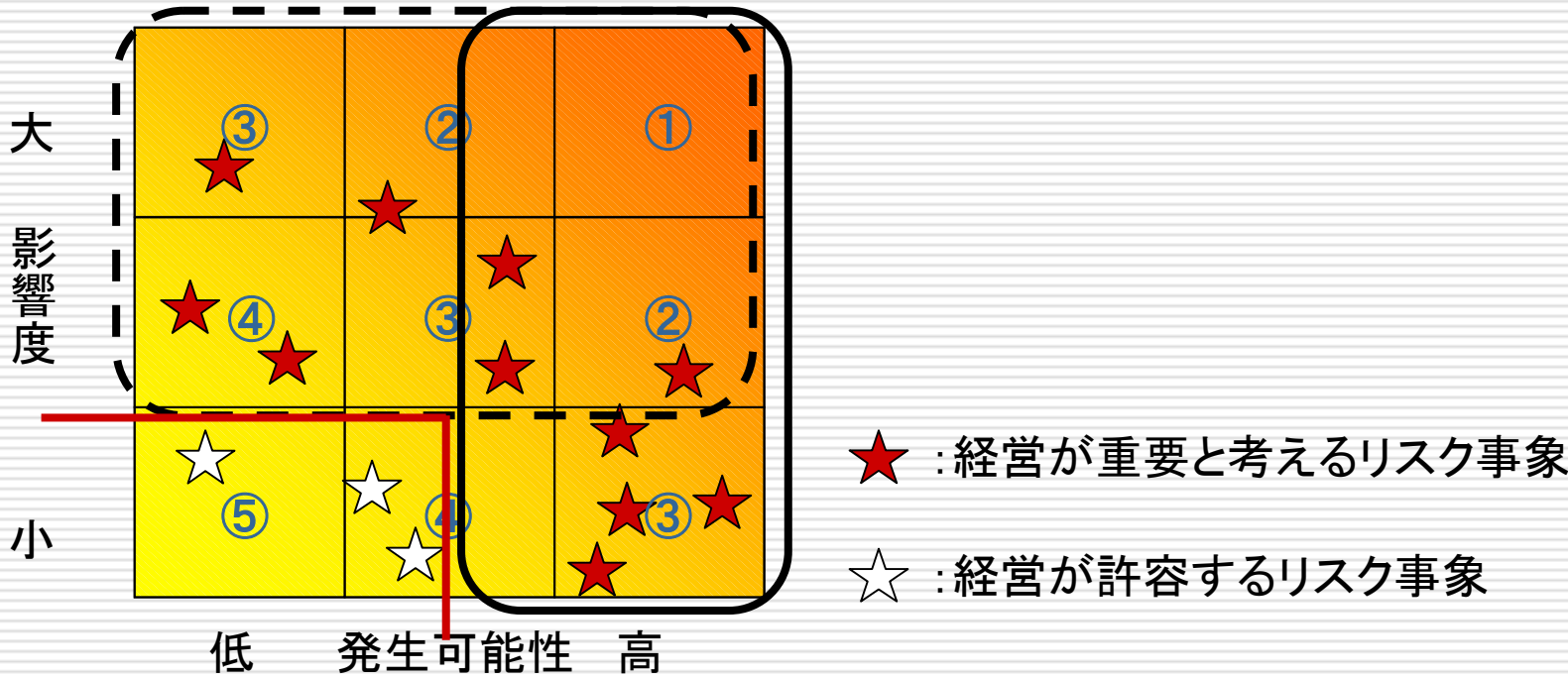
- オペレーショナル・リスクを計量化することを前提に「影響度」を金額ベースで評価する。
  - それぞれの「発生可能性」の想定(〇年に1回)を置く。
    - 潜在的なリスクについては、「影響度」、「発生可能性」ともある程度、割り切って想定を置かざるを得ない。
- (例)

リスク内容	影響度			発生頻度	統制上の改善点
	直接費用	間接費用	その他		
市場取引のオペミス	〇円	〇円		〇年に1回	×××××
顧客情報の漏洩	△円	△円	顧客の信用を毀損	△年に1回	×××××
自然災害	◇円	◇円		◇年に1回	×××××
内部不正	●円	●円	顧客の信用を毀損	●年に1回	×××××
⋮	⋮	⋮	⋮	⋮	⋮

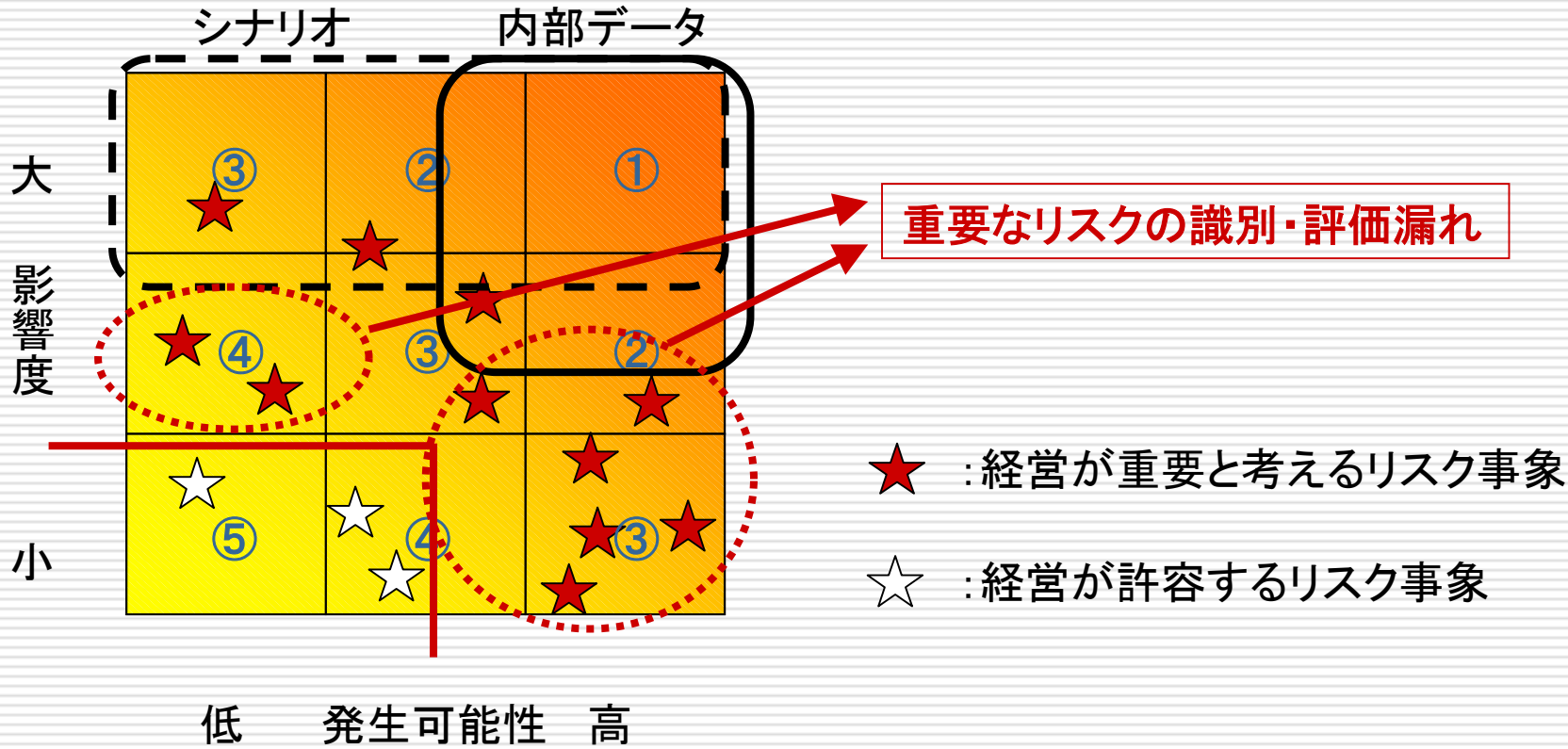


# 経営にとって「重要なリスク」の網羅的な把握

- 内部データとシナリオの組み合わせにより、「経営が重要と考えるリスク」を漏れなく、識別・評価する。



# 「重要なリスク」の識別・評価に漏れがあるケース



## 「重要なリスク」を網羅的に把握するための工夫

- 潜在的なリスクを含めて識別・評価する以上、1度の作業で「重要なリスク」を網羅的に把握するのは容易ではない。
- また、内外の環境変化等に応じ、経営にとって「重要なリスク」は変化し得る。
- したがって、リスク事象データの登録・蓄積を続けるとともに、CSAの定期・随時更新を行う必要がある。
- 他の金融機関で発生した事例（外部データ）の活用も有効。

（例）

- 金融庁行政処分事例（HP掲載）
- 新聞等での公表情報
- 他の金融機関との情報交換
- ベンダー提供の外部データ（海外事例が中心）

## リスク評価の客観性を高める工夫

実務に精通した複数名の担当者を選定し、影響度、発生可能性の評価を行う。

➤ 評価者個人の主観による評価を避ける観点から複数名によるエキスパート・ジャッジで評価を行う。

■ リスク統括管理部署がファシリテーターとなって、実務に精通した担当者を集めてワークショップを開催し、リスク評価を行う。

➤ リスク評価に漏れがないか、あるいは、組織横断的にみて評価の不整合はないか、を検証する。

■ なお、リスク評価に関する見解が分かれた場合には、多数決で決定する金融機関が多いが、少数意見をリスクコントロールマトリックスの備考欄に記入するケースもみられる。

## リスク評価の範囲の多様性

### データ・ベースの登録件数

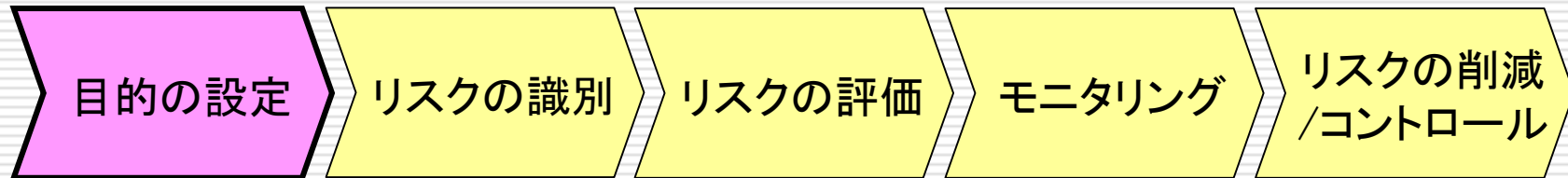
- 登録対象を一定金額以上の実損が発生した事件・事故に限定し、事務ミスなどは含めないケースであれば、月間登録件数は数件程度に止まる。
- 一方、事務ミス、顧客トラブル等も、可能な限り含めて登録対象としているケースであれば、月間登録件数は数百件に膨らむ。月間千件を上回る規模の登録がある地域金融機関も存在。

### シナリオの作成件数

- 本格的にCSAを導入した先では、数百～数千本(メガバンクでは、数万本)のシナリオのリスク評価を実施している。
- 試行的にCSAを導入した先では、数十～数百本のシナリオのリスク評価を実施している。

## リスクの識別と目的の確認

---

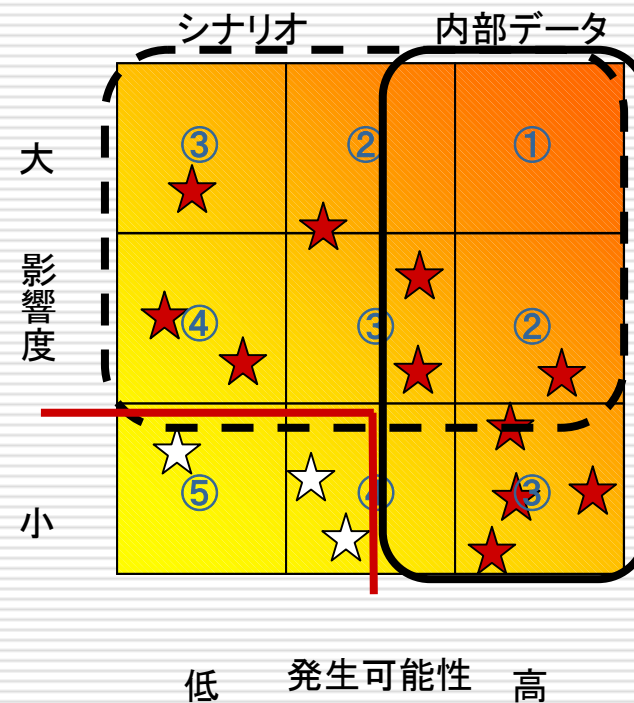
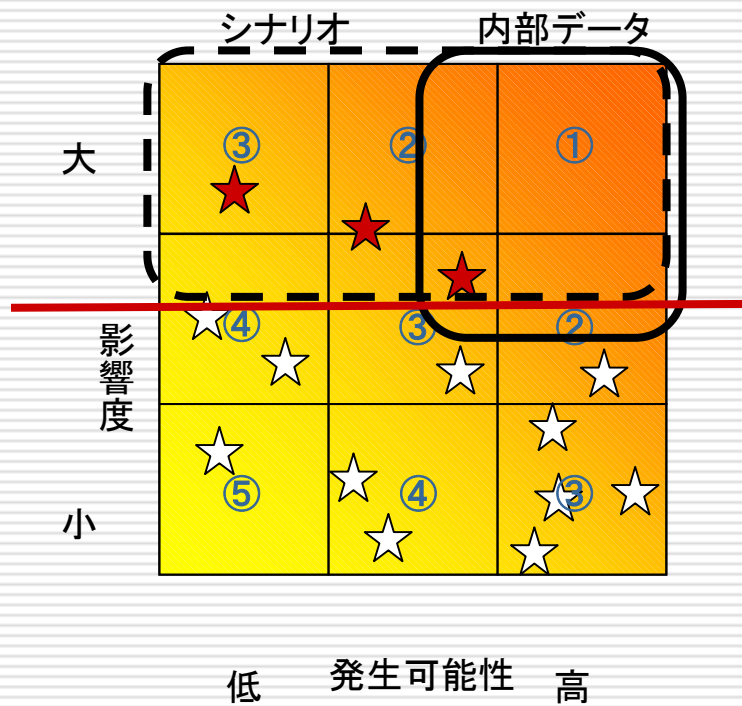


- 「リスク」とは、「目的」の達成に影響を与える事象発生の可能性。「目的の設定」がリスクマネジメント・プロセスの起点となる。
- 「重要なリスク」とは何かに迷ったら、「目的」は何かを確認するのが有効。
  - 何のためにリスクマネジメントをしているのか、に立ち返って考える。
    - 経営を揺るがすリスクへの備えを確認するためなのか
    - 業務プロセスの改善を図るためなのか
- 経営陣と継続的な協議を行うことも重要。

# 目的の違いとリスクの識別・評価の多様性

経営を揺るがす大きなリスクへの対応ができているかを確認したい

脆弱な業務プロセスの改善を図りたい

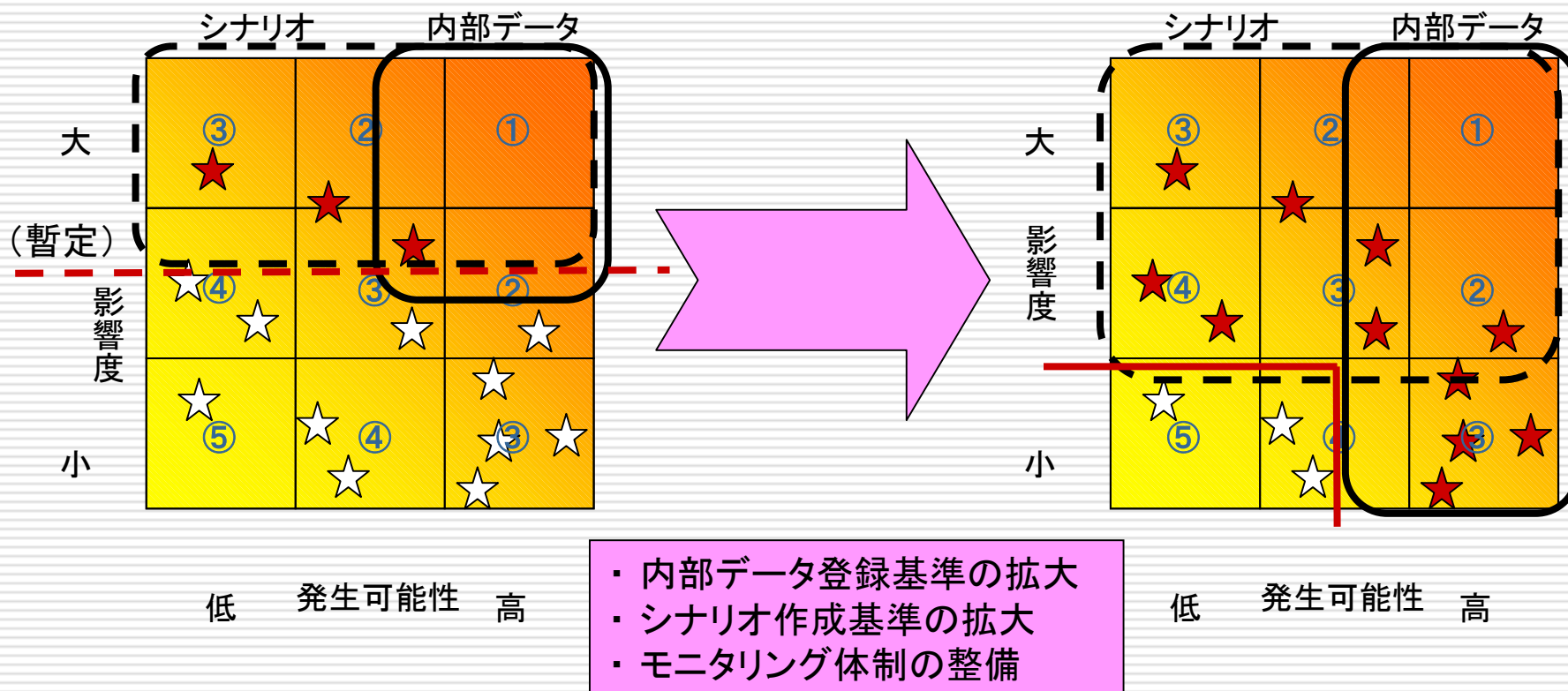


★ : 経営が重要と考えるリスク事象

☆ : 経営が許容するリスク事象



観点を变え  
対象を小さくはじめ、徐々に拡大していく方法もある。

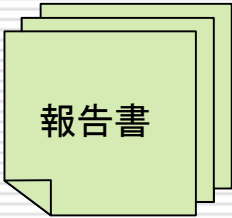


★ : 経営が重要と考えるリスク事象    ☆ : 経営が許容するリスク事象

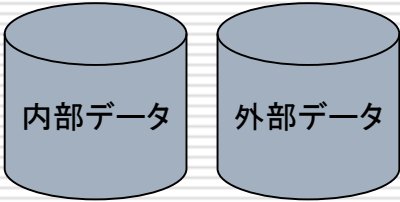


# (3) モニタリング

- オペレーショナル・リスク統括管理部署は、各リスク部署と連携して、組織全体のオペレーショナル・リスクの状況に関する様々な情報を収集する。
- また、膨大なモニタリング情報を収集、整理、分析して、オペレーショナル・リスク管理委員会等を通じ、経営陣に対し報告を行う。



- ・事件・事故報告
- ・事務ミス報告
- ・苦情トラブル報告

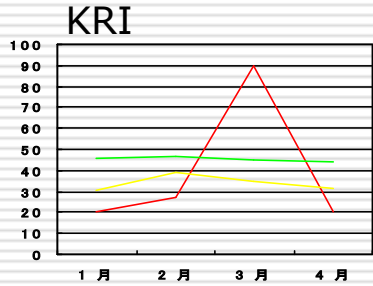


内部・外部データの分析

RCM

プロセス	リスクの内容	リスク分類	影響/リスクの発生	影響/発生頻度	コントロールの内容	種類	評価	残余リスクの対策	発生状況
123-001	業務ミス	大	大		定期的検査	大	大	1	
123-004	システム障害	中	中		定期的検査	中	中	2	
123-010	機密漏洩	小	小		不十分	小	小	3	
123-011	内部不正				24時間監視			4	
123-012	自然災害							5	
123-013	人為的災害								

CSAの定期更新・  
随時更新



各種指標(KRI)のフォロー

## Bad Newsをどのように集めるか

- ”Bad News” の伝達・共有に向けた働き掛け  
(例)
  - 経営トップによる訓示
  - 報告徹底に関する通達の発出
  - 内部データベースへの登録運動の展開
  - CSAの導入・定着のための啓蒙活動
- リスク管理部署あるいは内部監査部署による検証  
(例)
  - 個別報告は適時に行われているか
  - 個別報告やデータベースへの登録内容は正確か
  - CSAでは、リスクの洗い出し漏れがないか、評価は適切か
  - CSAは適時に更新されているか

## Bad Newsをどのように集めるか

---

- ”Bad News” の伝達・共有へのインセンティブ
  - 問題発生 の報告を受けた後、相応のスピード感をもって改善策の決定、実行に取り組み、その成果を組織内に示すことが重要。
  - 重要な事件・事故、顧客トラブル等の発生状況、原因分析などをフィード・バックすることも、報告者の納得感や報告のインセンティブを増す。
    - 反対に、事件事故、事務ミス の撲滅(ゼロ)運動や、過度な報告負担などは ”Bad News” を伝達・共有する際の障碍となったり、インセンティブを殺ぐこともあるので要注意。

## モニタリング情報の収集、整理、分析

---

### (個別リスク事象の報告)

- 発生部署からの第一次報告では、実態の把握や原因の特定が不十分なケースも少なくない。モニタリング部署は報告内容の検証を行う必要がある。
- 重要なリスク事象は、発生の都度、経営陣に個別報告を行う。軽微なリスク事象はまとめて報告を行うことも可。

### (内部データの登録・分析)

- 顕現化した重要なリスク事象をデータベース化する。
- 経営判断に利用する重要なデータ項目に関しては、モニタリング部署が検証(あるいは登録)を行う必要がある。
- 定期的に全体傾向をみたり、原因分析を行って経営陣、関係部署に報告を行う。

## モニタリング情報の収集、整理、分析

### (外部データの取得と活用)

- 他の金融機関等で顕現化した重要なリスク事象についても可能な限り、情報を取得してデータベース化する。
- 内部データと比較・検証したり、潜在的なリスクの洗い出し、評価等を行う際の参考とする。

### (CSAの定期・随時更新)

- 定期的にCSAの全体更新を行うとともに、その評価結果を経営陣に対し報告する(半期or年度に1回程度)。
- 自行あるいは他の金融機関で重要なリスク事象が発生した場合は随時、CSAを部分更新して、経営陣に報告する。
- 新規業務に取り組む前の段階で、CSAによる評価と経営陣に対する報告を義務付ける先も少なくない。

## モニタリング情報の収集、整理、分析

(KRIのフォロー)

- リスクの状況とその管理状況を表わす代表的な指標を KRI(= Key Risk Indicator)として選定し、その動向をフォローする。

▽リスクの状況(エクスポージャー、顕現化した結果)を表わす指標(例)

- |          |          |
|----------|----------|
| ・取引件数、金額 | ・事件・事故件数 |
| ・顧客数     | ・苦情件数    |
| ・取扱商品数   | ・事務ミス件数  |
| ⋮        | ⋮        |

▽管理状況を表す指標(例)

- ・要員数
- ・1人当たり事務量
- ・異例取引処理件数
- ⋮

## モニタリング情報の収集、整理、分析

- KRI指標の選定にあたっては、特に、以下の点に留意する。
  - リスク事象の発生件数・金額と、ある程度の相関関係が観察されること。
  - モニタリング指標としての客観性があること（自己申告ベースではないものが望ましい）。
  - 定期的に取得可能な指標であること。
  - 指標の算出にあまり時間が掛からないこと。
  - 組織として共有する意義のある指標だと認められること。
  - 指標数を管理可能な範囲内に抑えること。

## モニタリング要員の育成・確保

- オペレーショナル・リスクのモニタリング要員には、経営判断をサポートし得る、実務知識と分析力を身に付けることが求められる。
  - モニタリング情報を漏れなく、正確に収集する。
  - 膨大なモニタリング情報から、経営者の目線でみて、重要な情報を収集、整理、分析し、適宜、経営陣に報告する。
- 各業務・リスクカテゴリーに精通したモニタリング要員を育成・確保するとともに、連携して経営陣をサポートする体制を整備するのが望ましい。
- オペレーショナル・リスクのモニタリング要員の育成・確保には時間が掛かる。組織全体として、モニタリング要員の育成に、計画性を持って取り組む必要がある。



## (4) リスクの削減/コントロール

- オペレーショナル・リスクに関する諸情報をオペレーショナル・リスク管理委員会に集め、問題点を組織内で共有するとともに、対応策を協議、検討する。
- このとき、組織としては、少なくとも、以下の点について確認し、対応策の実施に関して合意することが重要。
  - ① コントロールの設計・導入の適切性
    - 問題点の是正、解消に繋がる有効な対応策であること
  - ② 費用対効果
    - 対応コストについて、経営が許容し得る範囲内にあること
  - ③ 優先順位
    - 組織内で、各種対応策の優先順位について合意を得ること

## 適切なコントロールの設計・導入

---

- リスク事象に関する実態把握が不足したり、発生原因の分析が不十分な場合、コントロールの設計・導入が適切性を欠くことがある。  
例えば、実効性のない注意喚起の本部通達が多用されたり、コントロールの過剰な設定を招くことも少なくない。
- オペレーショナル・リスクの場合、1つのリスク事象に対して、複数のコントロールを導入することも多い。  
1つ1つのコントロールの意義・目的や、コントロール体系の中での位置付け(キー・コントロールか否か)等をよく考えて、適切なコントロールの設計・導入を検討すべきである。

## 適切なコントロールの設計・導入

### ▽意義・目的からみたコントロールの種類

	意義・目的	具体例
予防的コントロール (Preventive Control)	リスクの顕現化を防止・抑制する。	稟議書の本部承認 役席カードによる取引承認 窓口・出納・渉外の分離 フロント・バックの分離 金庫、オープン出納機、鍵管理機の導入
発見的コントロール (Detective Control)	顕現化したリスク事象を発見・是正する。	事後検印 残高チェック 自主点検、自店検査
指揮的コントロール (Directive Control)	リスク認識を高め、行動規律の徹底を促す。	経営理念、企業憲章 心得、ガイドライン 経営トップによる訓示、注意喚起の本部通達 事務ミス削減運動 研修

## 費用対効果の勘案

- オペレーショナル・リスク管理委員会において、定期的に問題点と対応策をリストアップ。問題点と対応策を横並びに比較することで、組織内で整合性のとれた解決策に導く。  
(評価の目安)
  - リスクの重要度からみて、対応策の優先順位は適当か
- 可能な範囲で、対応コストと効果を評価して、対応の可否、優先順位を協議し、合意を得る。  
(評価の目安)
  - 対応コストが、経営として許容し得る範囲内に収まっているか
  - 他の対応策と比較して、対応コストが過大ではないか

## 規律重視の組織文化の醸成

### (オペレーショナル・リスクの特徴⑦)

- オペレーショナル・リスクは、組織内のすべての役職員が関係する。組織文化によっては、決められたコントロールが徹底されないことがある。



### (オペレーショナル・リスクの管理のポイント⑦)

- オペレーショナル・リスクを管理するためには、組織・体制や管理手続きを整備するだけでは不十分であり、規律重視の組織文化の醸成に努める必要がある。

## 規律重視の組織文化の醸成



バーゼル銀行監督委員会  
「オペレーショナル・リスクの管理と監督に関するサウンド・  
プラクティス」(2003/2)

- 取締役会および上級管理職の双方には、効果的なオペレーショナル・リスク管理に高い優先順位を置き、健全な業務コントロールに徹する**組織文化**を作る責任がある。
- オペレーショナル・リスク管理は、銀行の全てのレベルにおいて、**銀行の文化**が高い倫理行動基準に重点を置いているときに最も効果を発揮する。
- 取締役会および上級管理職は、行動と言葉で、全職員が正しく銀行業務を遂行することへの期待を形成するような**組織文化**を醸成すべきである。

## 規律重視の組織文化の醸成

### ① 指揮的コントロール(Directive Control)の効果的な活用

- オペレーショナル・リスクの管理は、最終的には組織体に属する役職員1人1人のリスク認識、行動規律の問題に帰着する。
- このため、多くの金融機関では、従来から、役職員のリスク認識を高め、行動規律の徹底を働きかける目的で、経営トップによる訓示、注意喚起の本部通達、心得・ガイドラインの制定、研修などを実施している。
- 上記のような指揮的コントロールは、総花的、抽象的になりがちであるが、実効性を高めるためには、重要なリスクは何か、キー・コントロールは何かを具体的に明示して、役職員全員で共有することがポイント。

## 規律重視の組織文化の醸成

### ② 営業店CSAの活用

- 近年、営業店のリスク認識、行動規律の徹底を促す観点から、営業店CSAに取り組む金融機関が増加している。

CSA評価 (問題点)	コントロール 強化策	進捗状況			取組結果	本部評価
		○月	○月	○月		

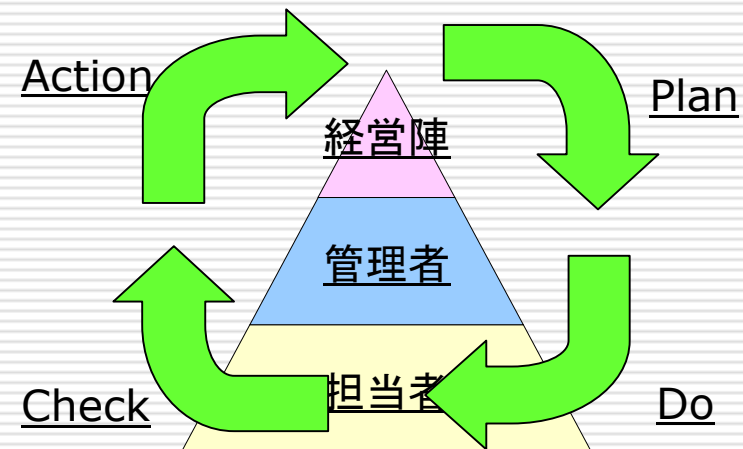
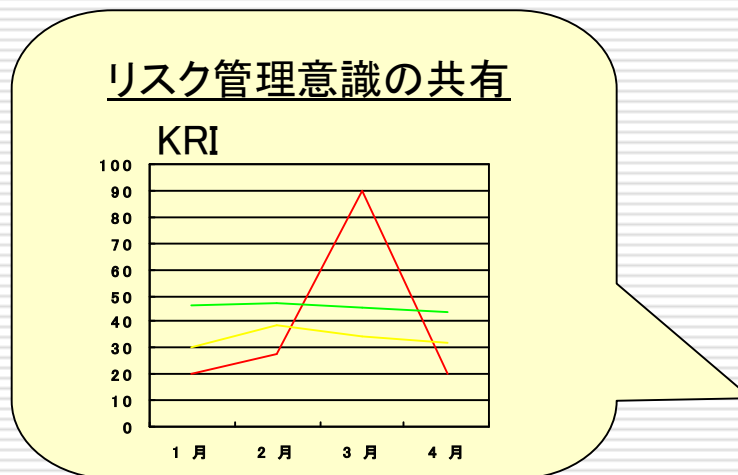
- 質問書形式。所管のリスク管理部署が各営業店に対し、リスク・コントロールマトリックスの作成を依頼。
- 各営業店が、自主点検などを通じて、自ら改善を要すると判断した業務プロセスを評価対象に選定。各営業店が自ら、改善策を策定し、定期的に所管のリスク管理部署に改善状況を報告する。



## 規律重視の組織文化の醸成

### ③ KRI指標の活用

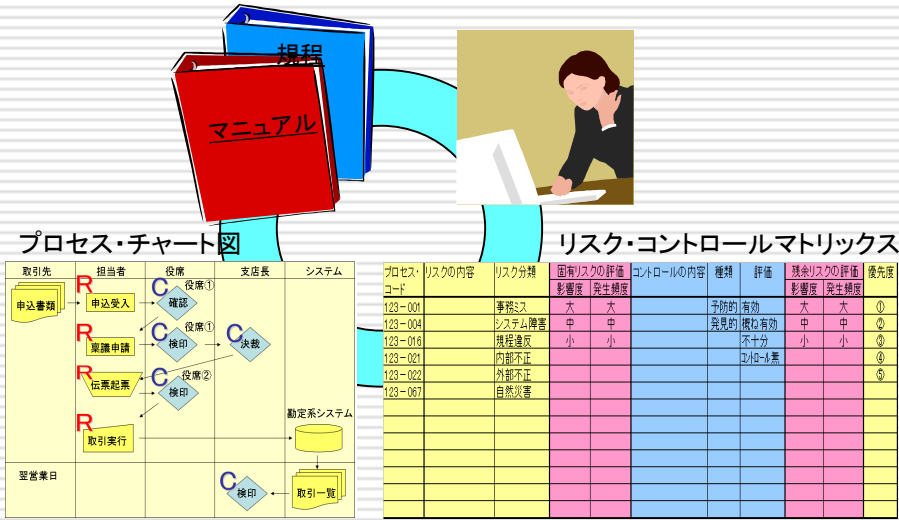
- 経営陣から営業店の担当者にいたるまで、オペレーショナル・リスク管理の意識を共有するため、代表的なKRI指標を選定・モニタリングして、経営陣に報告するとともに、現場にもフィードバックを行う金融機関もみられる。



# 規律重視の組織文化の醸成

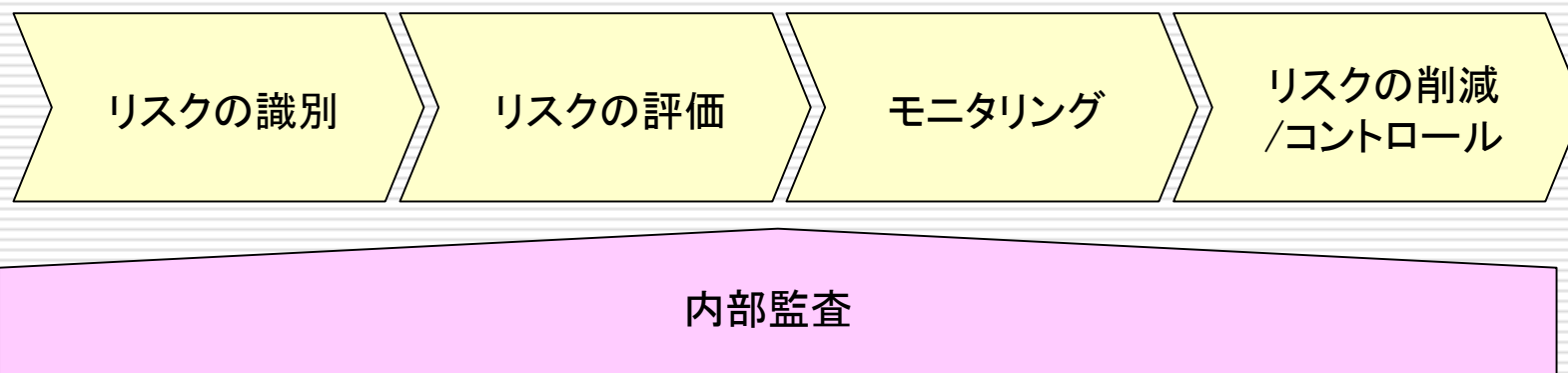
## ④ 内部統制フレームワークの共有

- 例えば、日頃、職員が参照する機会の多い「**規程・マニュアル類**」と「**プロセス・チャート図**」、「**リスク・コントロールマトリックス**」を電子化。
- この「**3点セット**」を、常時、行内ネットワークで閲覧可能な体制を整備し、各業務に従事する役席・担当者の**リスク認識**や**内部統制**に関する意識の向上を促す**金融機関**もみられる。



## 4. 内部監査による検証

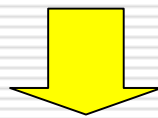
- 内部監査では、リスク管理の実態を踏まえて、検証の重点ポイントを選定し、オペレーショナル・リスク管理の実効性を高めるように促していく。
- 基本フレームワークの導入段階と定着段階では組織全体に内部監査の実施が与える影響が異なる点に留意する。
  - ー 導入段階で厳しい内部監査を実施すると基本フレームワークの定着にマイナスの影響を与えることもある。



## 5. 更なる高度化に向けての課題

---

- ◆ 多くの金融機関が、オペレーショナルリスク管理の実効性を上げるために、全社的な組織・体制を整備するとともに、バーゼル銀行監督委員会が提示した基本フレームワークの導入などに取り組んできた。
- ◆ オペレーショナルリスク管理の高度化に対して、先行して取り組んできた金融機関では、当初目的を概ね達成し、より実効性のあるオペレーショナルリスク管理の方策を模索し始めている。



- ◆ オペレーショナルリスク管理の取り組みは次のステージへ

## 基本フレームワークの導入先が感じている限界

---

- ① 重要なリスクを網羅的に把握できているか？
- ② 影響度や発生可能性を客観的に評価できているか？
- ③ (一部先)計測されたリスク量は信頼できるのか？
- ④ 自らのリスクプロファイル、業務プロセスの脆弱性などの把握・分析はできているか？

## 最近のデータ・シナリオ共有化への取り組み事例

---

- ◆ 地域金融機関 数行が、自主的にデータ交換、シナリオ交換を開始。

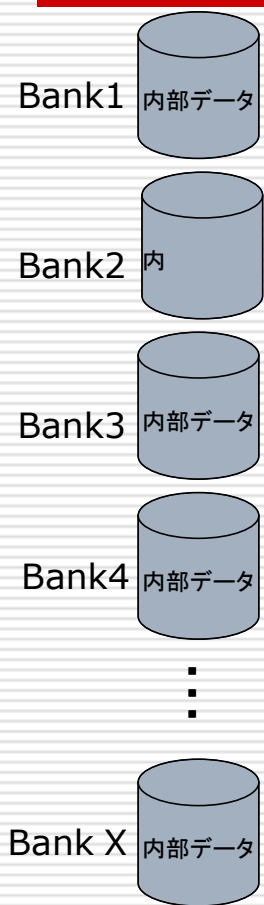
- シナリオの交換
- 内部データの交換
  - ・ 集計値、傾向値
  - ・ 個別データ

〔主要登録項目のほか、銀行情報・個人情報を  
マスキングして概要を記載〕



- ◆ 上記取り組みを契機にして、データ・コンソーシアムの設立機運が高まった。

# データ・コンソーシアムの活用可能性

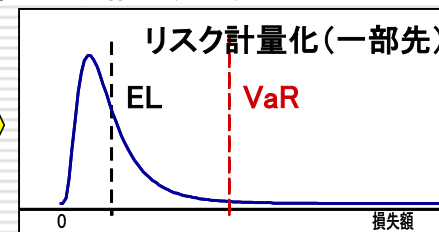


データ・コンソーシア

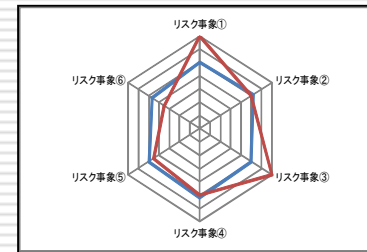
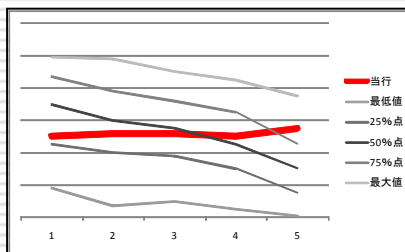


## ①重要なリスク事象の把握・評価： 網羅性、客観性の向

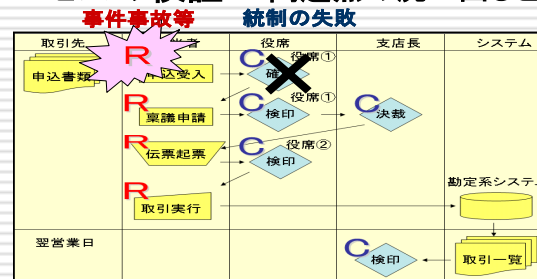
カテゴリ	リスク事象区分	事例(概要)	件数	金額	当行登録
事務リスク	XXXX	XXXX XXXX	XX件	XXX 円	○(有)
	為替事故(送込債・処理遅延等)	XXXX XXXX	XX件	XXX 円	×(無)
		XXXX XXXX	XX件	XXX 円	×(無)
システムリスク	XXXX	XXXX XXXX	XX件	XXX 円	×(無)
	XXXX				
法的リスク	XXXX				
人的リスク	XXXX				
有形資産リスク	XXXX				
その他のオペリスク	XXXX				
	XXXX				



## ②データ分析の高度化： リスクプロファイル、強み・弱みの把

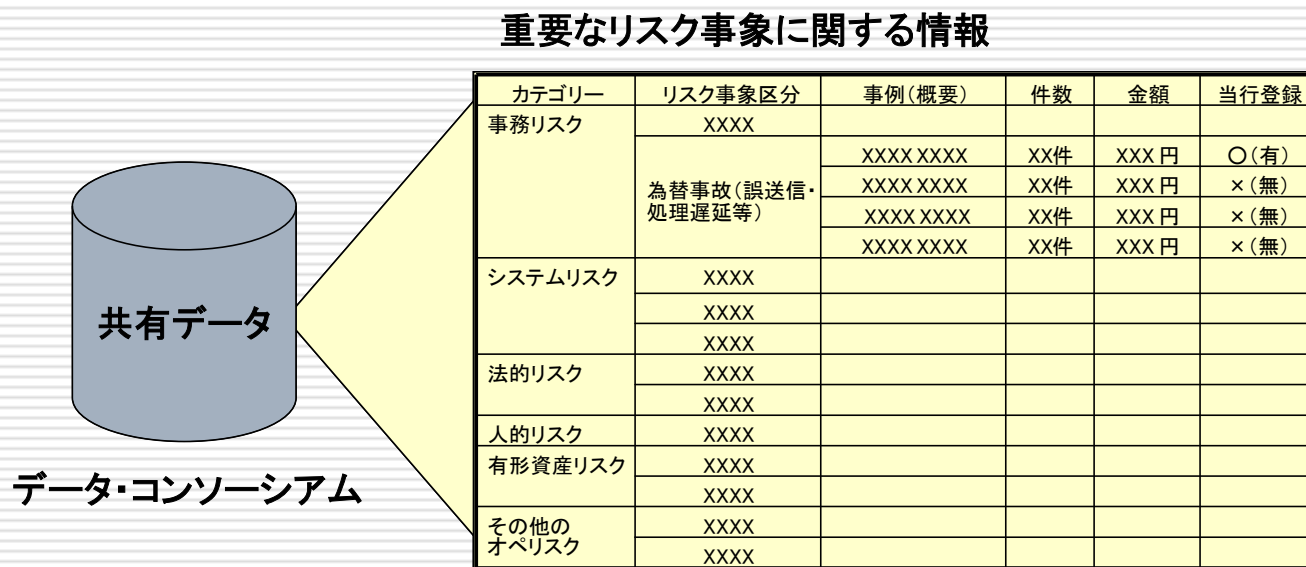


## ③業務プロセスの検証： 問題点の洗い出しと対応策の検討



# ① 重要なリスク事象の把握・評価

- ◆ 多くの金融機関がデータ・コンソーシアムに参加し、データの蓄積が図られることによって、「重要なリスク事象」を網羅的、客観的に把握、評価することが可能となる。





## 重要なリスク事象の網羅的な把握

---

- ◆ 重要なリスク事象としては、どのようなものがあるかを網羅的に把握できる。

(重要なリスク事象の例)

- ① 発生件数の多いリスク事象
- ② 発生時の損失金額の大きいリスク事象
- ③ 当該金融機関では起きたことはないが、

他の金融機関で実際に起きたリスク事象

- ◆ これまで④最近、新たに発生し始めたリスク事象  
シナリオを作成したことのない金融機関でも、  
オペレーショナル・リスク管理の高度化に取り組みやすくなる。

## 重要なリスク事象の客観的な評価

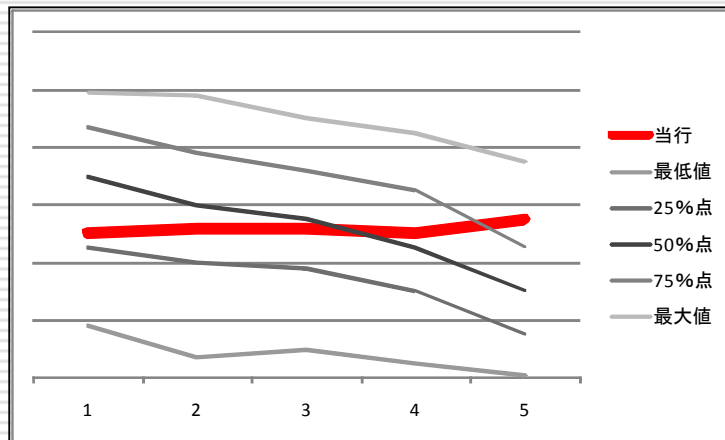
---

- ◆ 多くの金融機関のデータが集まれば、同一のリスク事象の発生可能性や影響度(損失予想)を客観的に評価することができる。
  - 例えば、100金融機関が参加し、10年間のデータ蓄積が進んだとすると、過去1回、発生したリスク事象の発生可能性を0.1%程度と見積もることができる。
  - 損失金額についても、規模調整等を行う必要はあるが、客観的事実にもとづいて評価することが可能となる。
- ◆ リスク事象の発生可能性、影響度の評価に関して、客観性が向上すると、経営判断の際の重要情報として活用できる。
  - 計測したリスク量(VaR)についても信頼性が増し、経営判断に活用しやすくなる。

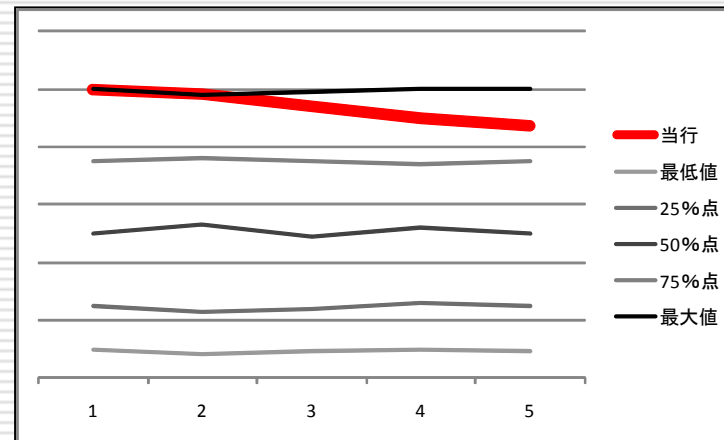
## ② データ分析の高度化

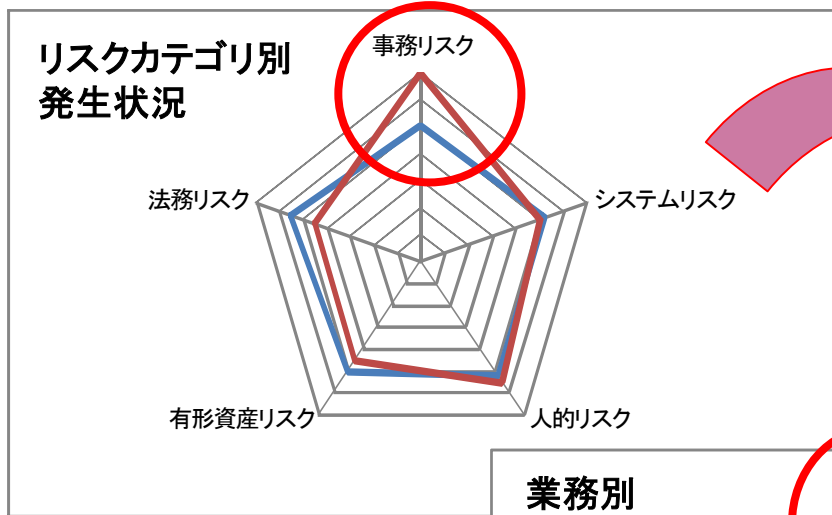
- ◆ 多くの金融機関のデータが集まれば、集計値・傾向値と比較することにより、自らのリスクプロファイルの特徴や統制面の「強み・弱み」などを把握・分析することができる。

(例)リスク事象①の発生状況

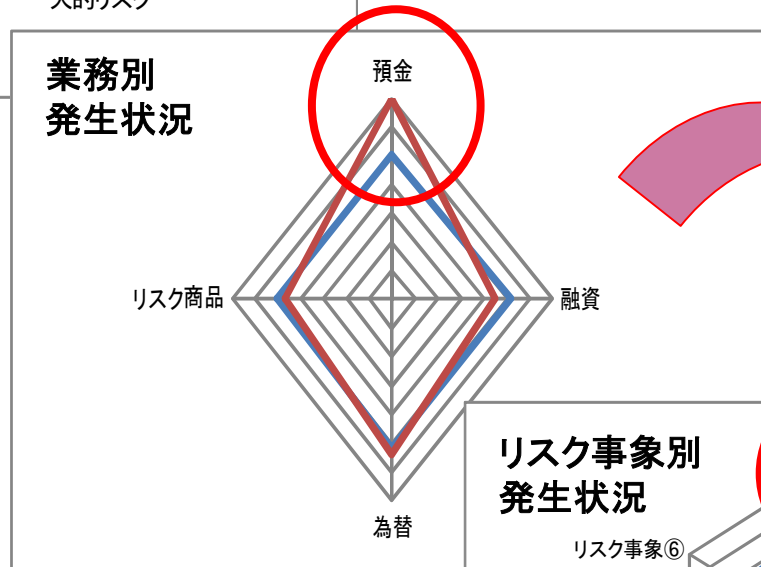


(例)リスク事象②の発生状況

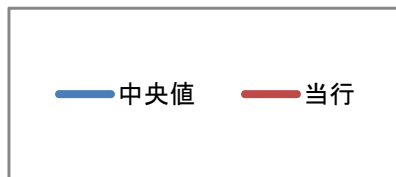
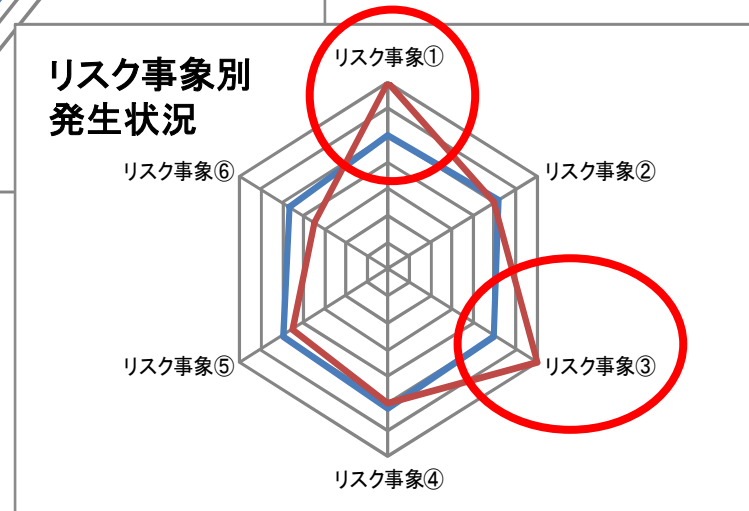




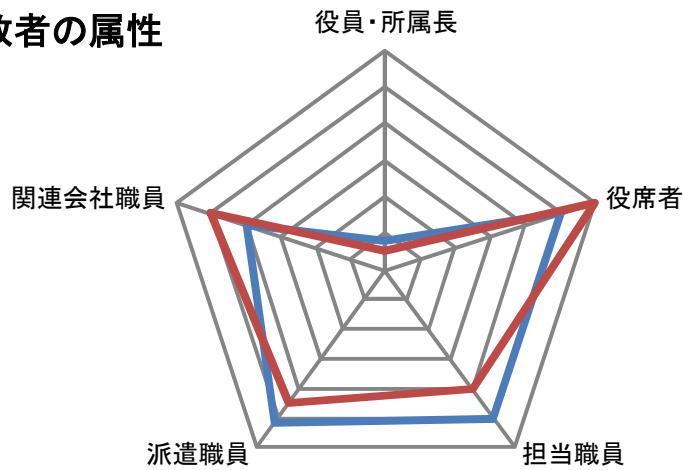
詳細分析(ドリル・ダウン)



詳細分析(ドリル・ダウン)



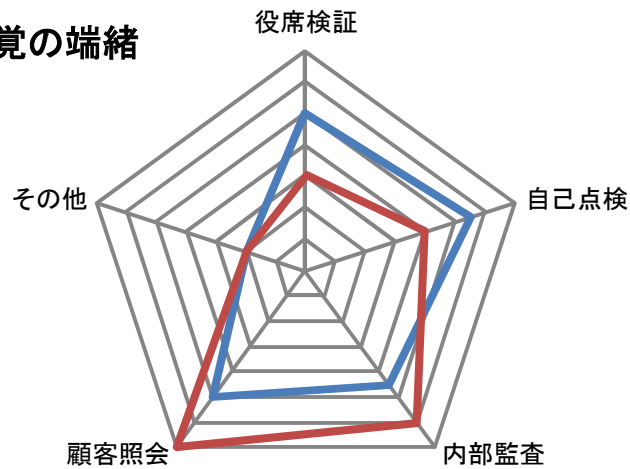
### 事故者の属性



事故者としては、担当者、派遣職員が少ない一方、役席者、関連職員が多い。

— 中央値 — 当行

### 発見・発覚の端緒



役席検証、自己点検よりも、顧客照会や内部監査で発見・発覚することが多い。

— 中央値 — 当行

## (留意点) 登録データの標準化

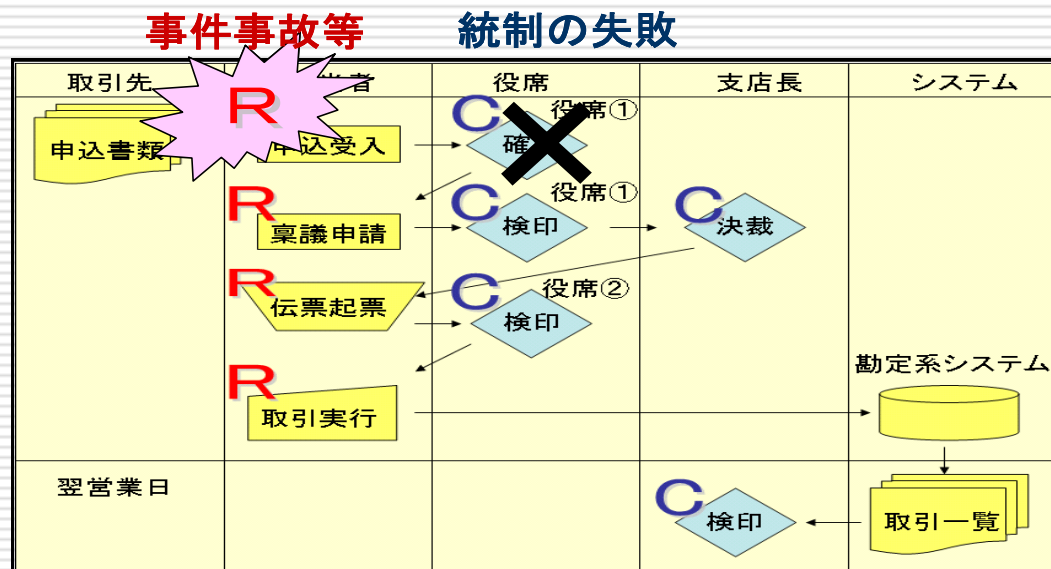
---

- ◆ 管理目的の違いや技術的な問題などから、金融機関の内部損失データの損失定義や収集基準は異なっている(スライド9,10参照)。
- ◆ 多くの金融機関のデータを集計・加工し、自行データと比較するためには、データの標準化を図る必要がある。

※ 重要なリスク事象を識別して、シナリオを作成したり、業務プロセスの検証を行う際にはこうした登録データの違いは格別問題にならない。

### ③ 業務プロセスの検証

- ◆ 重要なリスク事象を把握できれば、自らの業務プロセスにあてはめてみて、発生する可能性があるかを検証できる。
- ◆ 予め対応策を検討して、重要なリスク事象の発生を未然に防止することができる。

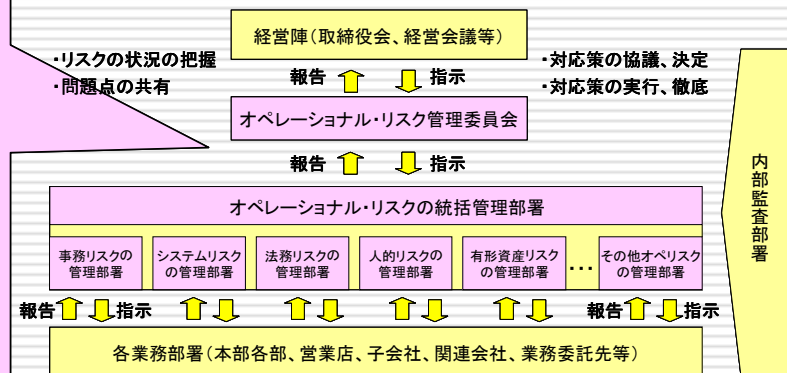


# リスク事象の事例研究とリスク・コミュニケーション

- ◆ データ・コンソーシアムに登録されたデータは、他の金融機関で実際に起きた事象であるため、シナリオの想定とは違ってリアリティがある。
- ◆ 経営陣やリスク管理部署、業務所管部署など、関係者間でリスク・コミュニケーションを行うときに「事例」として活用しやすい。

## オペレーショナル・リスク管理委員会

- ・他の金融機関では既に起きています！
- ・実際に●億円の損失が発生しました！
- ・私たちの金融機関でも起きる可能性があります！





---

(参考文献)

日本銀行金融高度化センター 碓井茂樹  
金融高度化セミナー資料  
「オペレーショナル・リスク管理の高度化のポイント」  
(2010年3月)  
「Q&Aオペレーショナル・リスク管理の高度化を巡る  
論点整理」(2010年3月)

日本銀行金融高度化センター 碓井茂樹  
ワークショップ資料  
「オペレーショナル・リスク管理の高度化-現状と  
今後の方向性」(2010年4月)