オペレーショナルリスク管理態勢の整備

2017年7月

日本銀行金融機構局
金融高度化センター

目　次

1．オペレーショナルリスクとは

定義

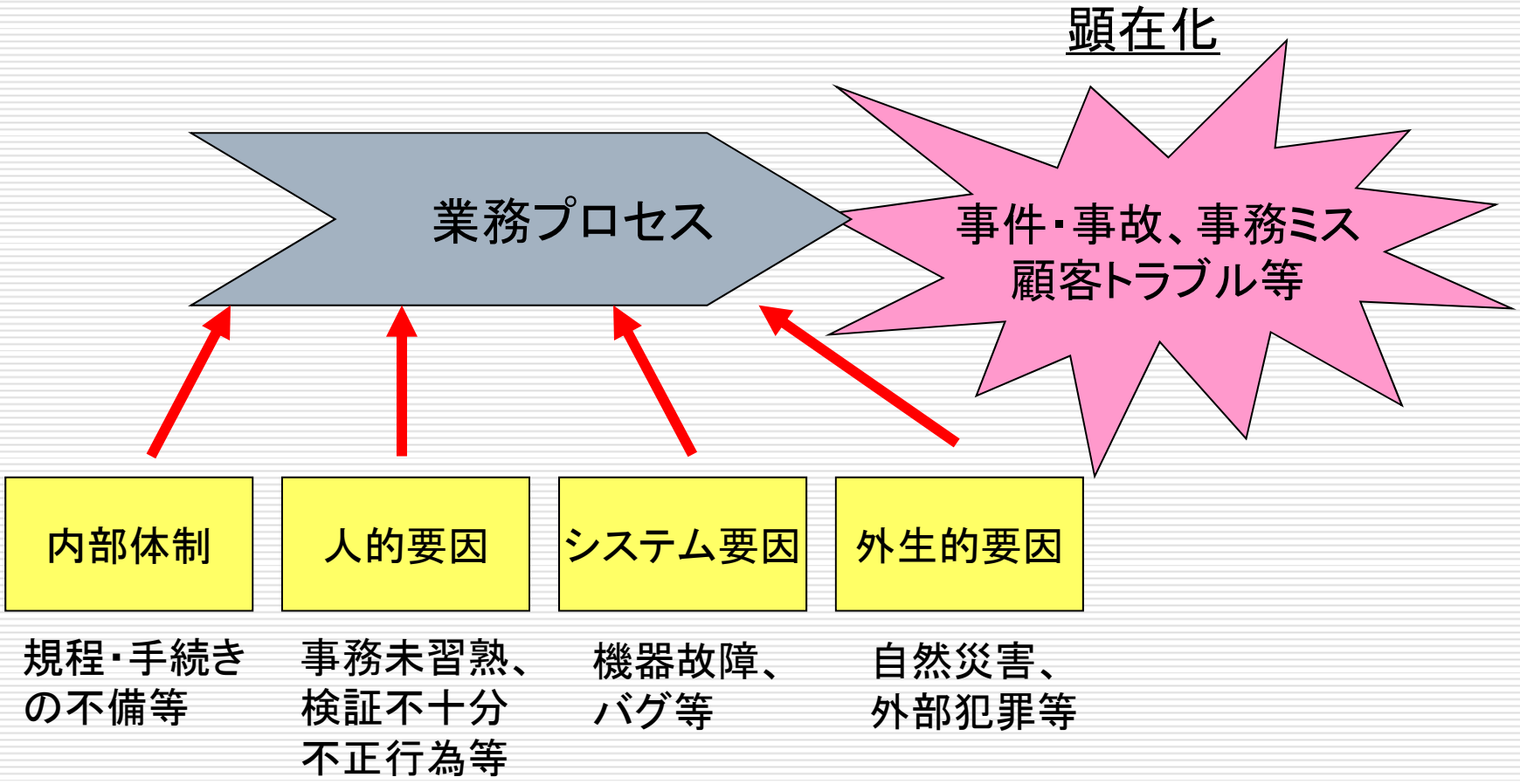
オペレーショナルリスクとは、
金融機関の業務の過程、役職員の活動、もしくはシステムが不適切であること、または外生的な事象により損失を被るリスク（規制自己資本比率の算定に含まれる分）

および、金融機関自らがオペレーショナルリスクとして定めたリスク（規制自己資本比率の算定に含まれない分）

をいう。

※ 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自らが定める。規制自己資本比率算定上のリスク計量化対象には戦略リスク、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・リスクの顕在事例

- 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・ローンダリング
  - インサイダー取引
  - システム障害
  - 情報漏洩・流出
  - 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
  - ⋮

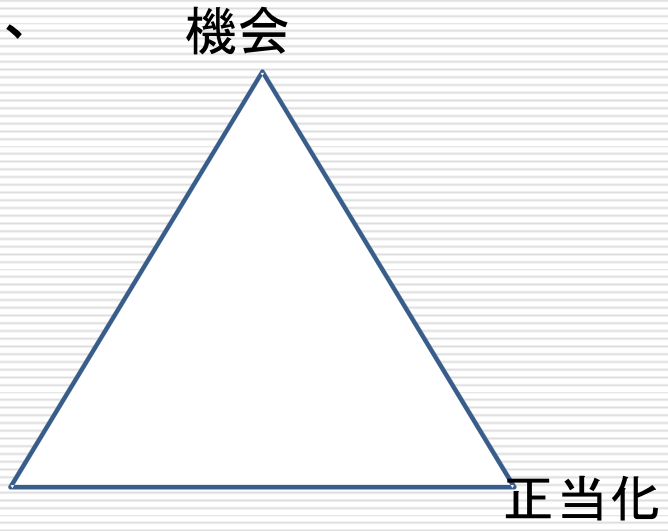
（参考１）クレッシーの不正のトライアングル

- 不正行為が起きる仕組みを説明する理論として、クレッシーの「不正のトライアングル」がよく知られています。
- この理論では、不正行為は

①不正行為が起き得る「機会」を認識し、

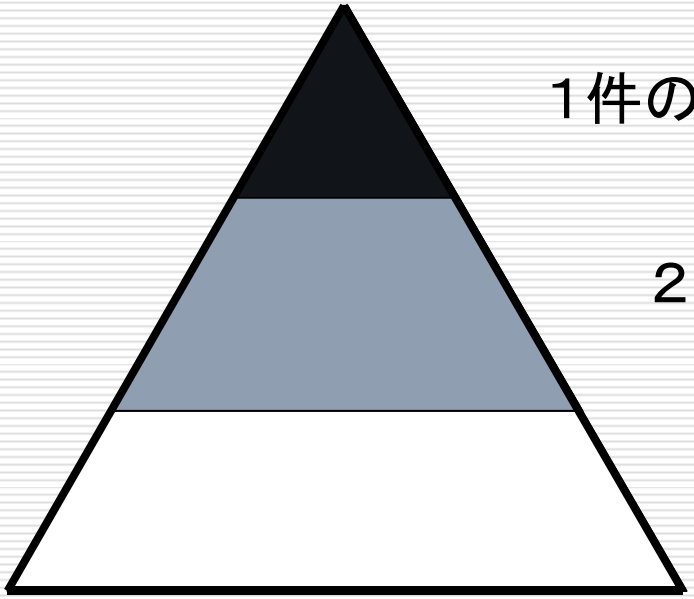
②不正行為に及ぶ「動機」を持つ者が、

③自分は不正を犯しても許される
はずであるという「正当化」理由
（言い訳）があると感じたときに
はじめて起きると考えられています。



（参考2） ハインリッヒの法則(トライアングル)

- 1つの重大事故の背後には 29の軽微な事故があり、その背景には300の異常が存在する。

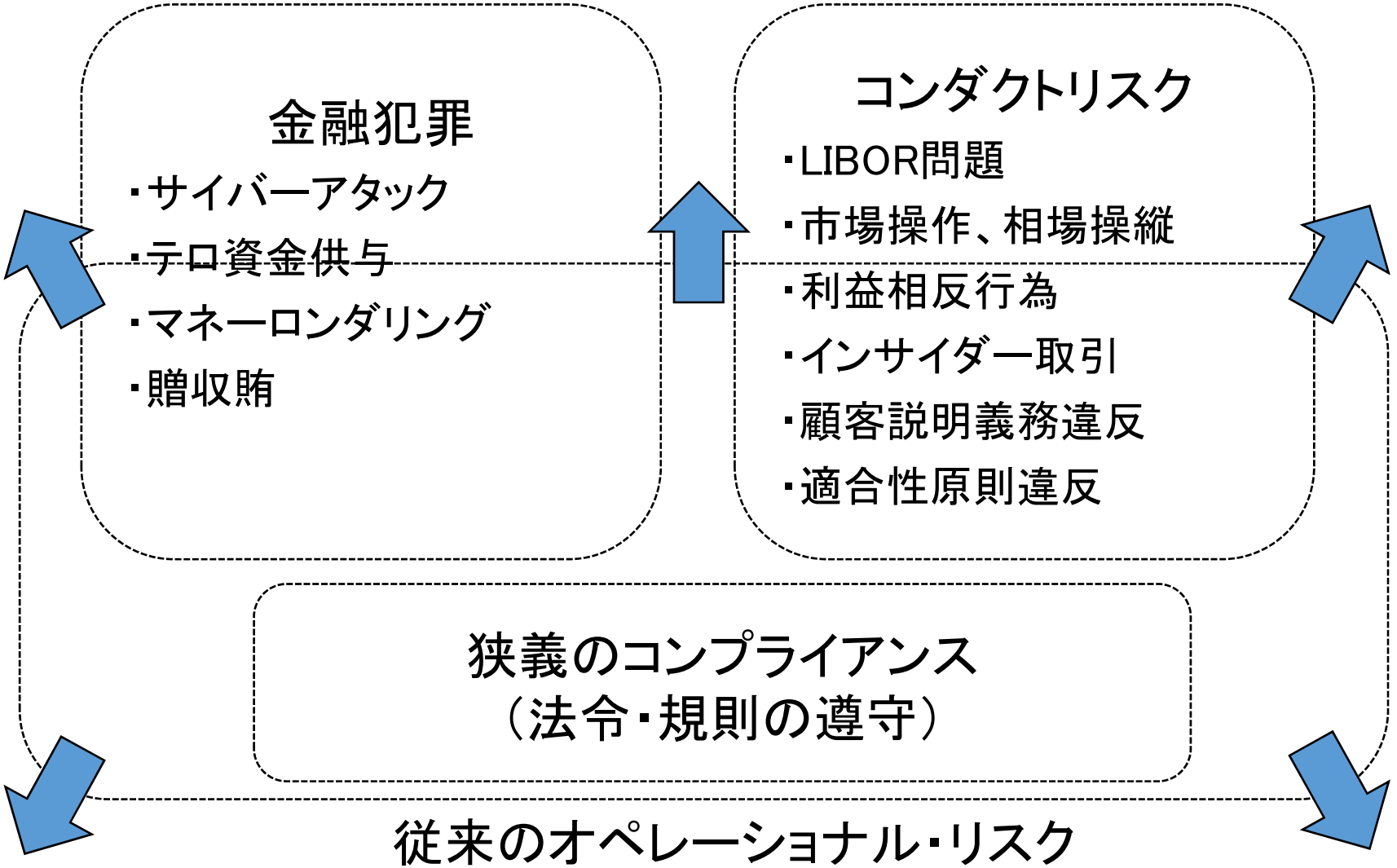


1件の重大な事故

29件の軽微な事故

300件のヒヤリ、ハット

拡大するオペレーショナル・リスク



（参考３）コンダクトリスク

- 英国金融当局（FCA※1）は、「顧客の正当かつ合理的な期待に応えることを金融機関がまず第一に自らの責務としてとらえて、顧客への対応や金融機関同士の行動や市場での活動で示すこと」を金融機関に期待されるコンダクトとして定義。
- 「顧客保護」、「市場の健全性」、「有効な競争」に対して悪影響を及ぼす行為が行われるリスクをコンダクトリスクとして定義している。※2

※1　FCA（Financial Conduct Authority 金融行為監督機構）：　国際金融危機を契機に英国において、金融サービス機構（Financial Service Authority：FSA）の解体を含む金融監督システムの見直しのなかで、新たに金融サービス分野における業務行為に関して責務を負う監督当局として創設。

※2　Journey to the FCA October 2012

従来のコンプライアンス、オペレーショナルリスクとコンダクトリスクはどこが違うのか

狭義のコンプライアンスとの違い

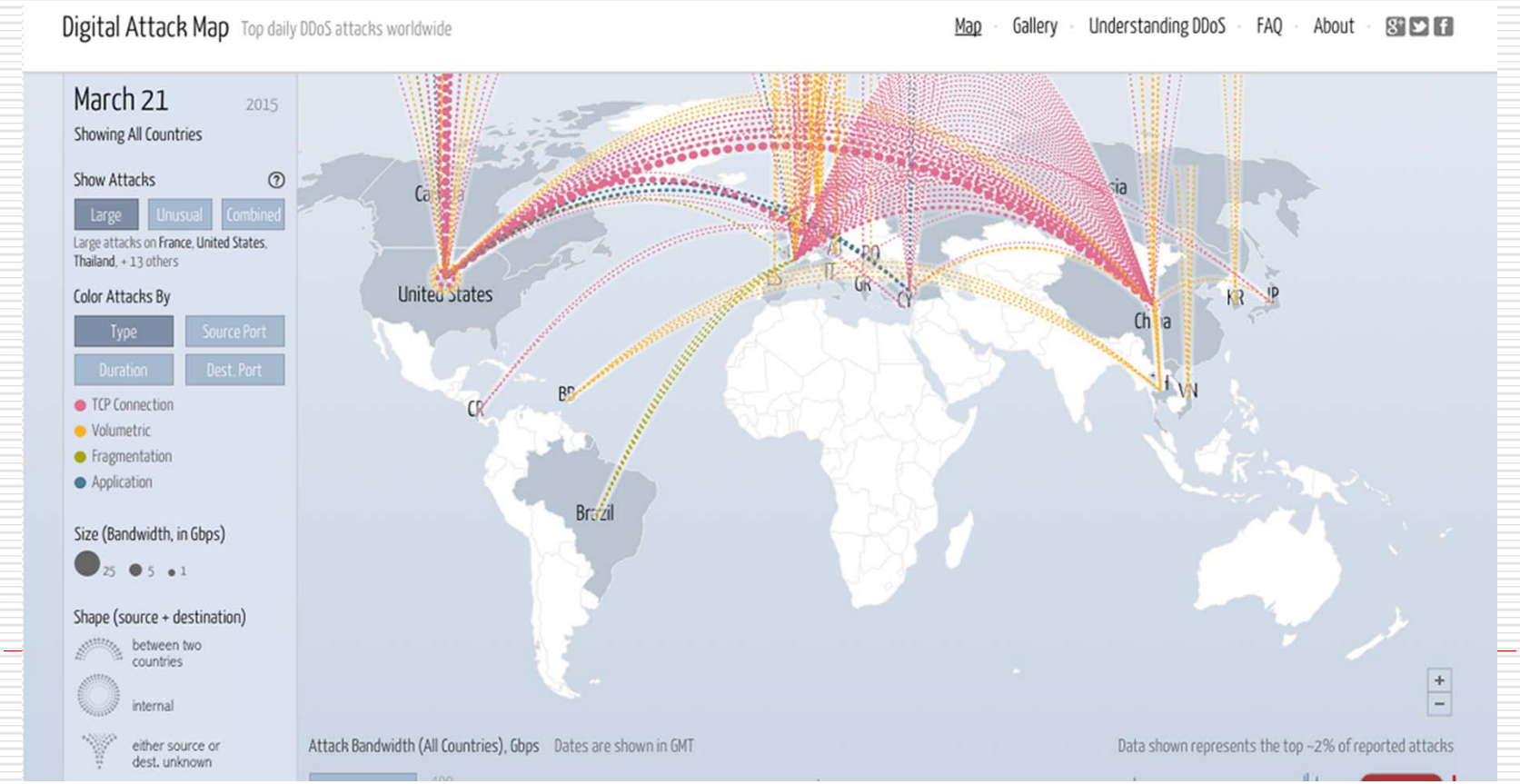
- 法令・規則に違反していなくても、社会規範に違反している。

従来のオペレーショナル・リスクとの違い

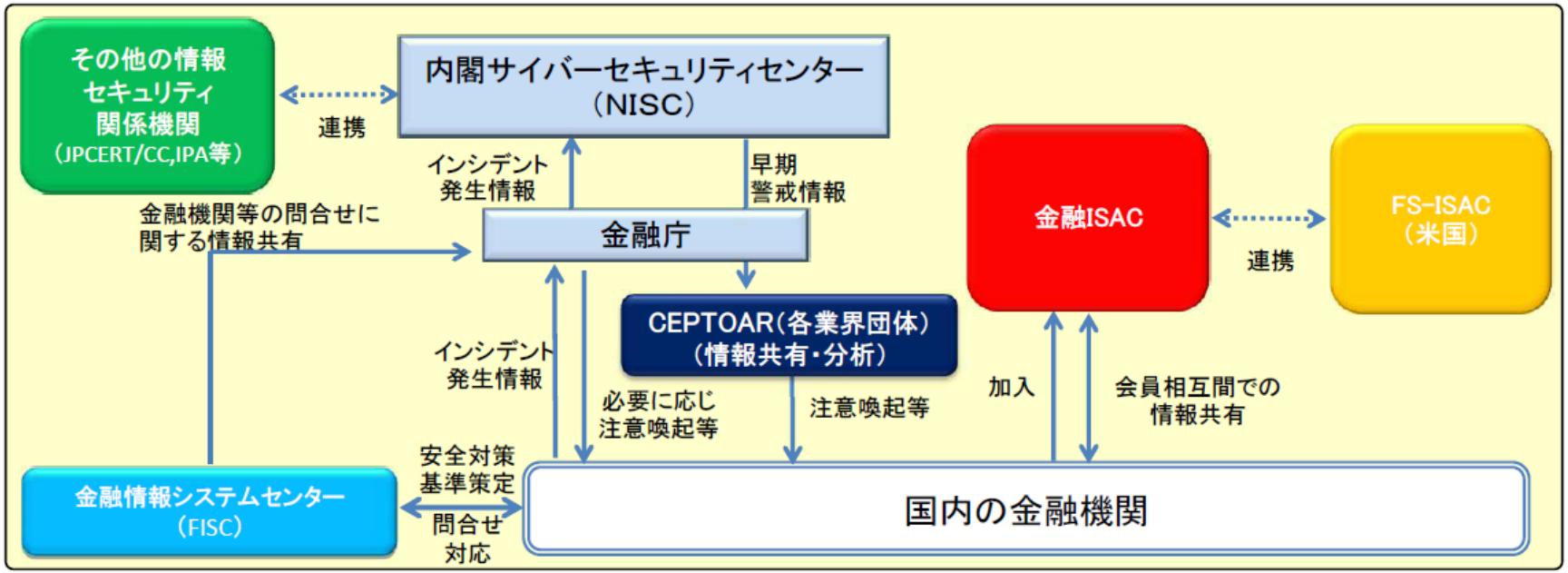
- 自社は直接損失を蒙らないが、顧客などの外部のステークホールダーが損失を蒙る。 自社は信用を毀損する。

（参考4）サイバーアタック

- D-DOS攻撃
- ロンサムウィルス
- WEB改ざん
- 標的型メール



組織犯罪にはセキュリティ関係者が連携して対応する必要



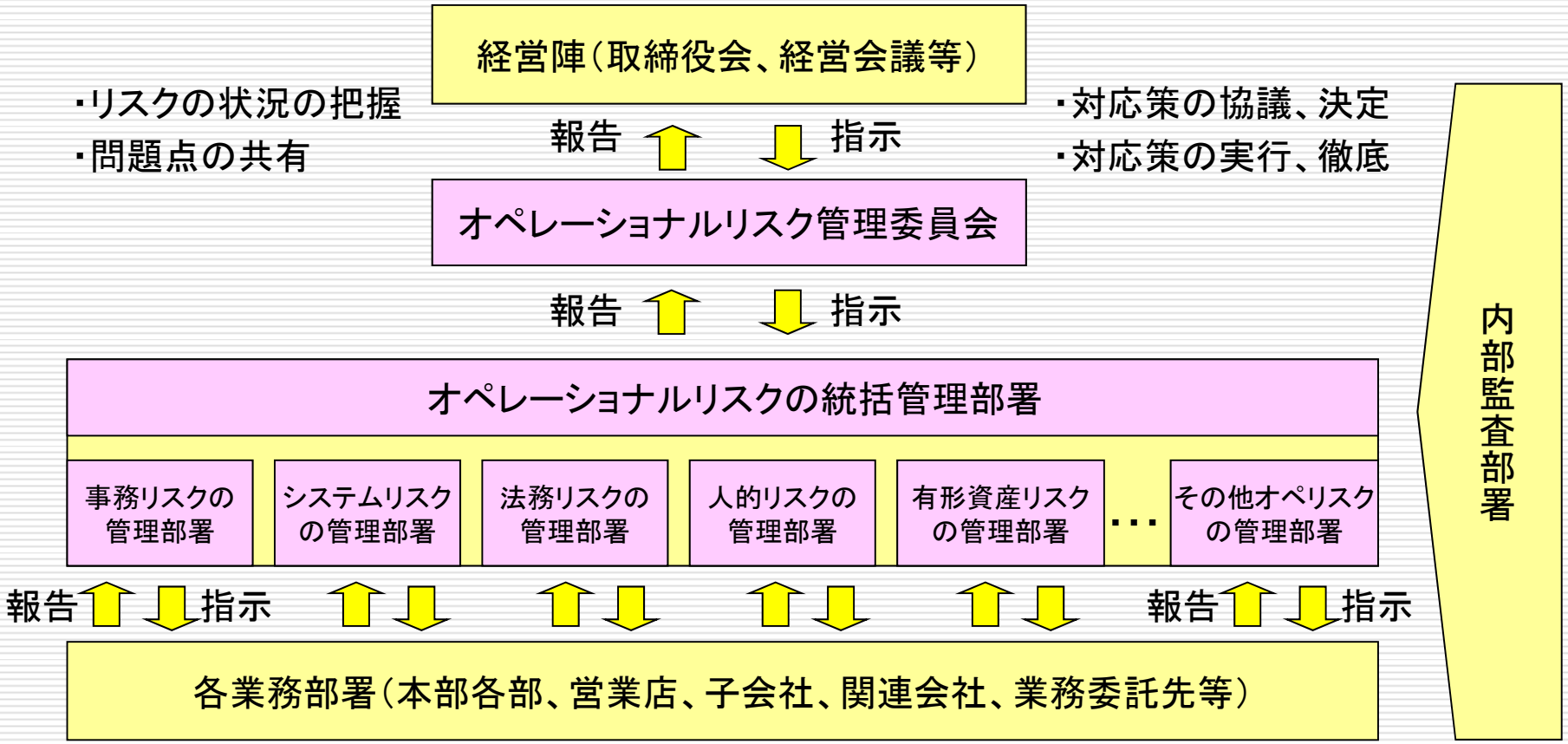
10月30日 (金)		10月31日 (土)	
		6:45~9:30 (時間自由)	朝ごはん
10:00	事前説明 ① チーム分け発表 ② 環境構築	10:00	⑤ 報告会
12:00	昼ごはん	12:00	昼ごはん
	③ レッドチームによる攻撃 ④ ログ解析 (インシデント対応)		⑥種明かし ⑦解説・講評 ⑧反省会
		17:00	撤収
19:00	晩ごはん		
??:??	解析終了（するといいね）		

金融ISACによる演習

レッドチーム

ブルーチーム

2. 組織・体制の整備



※ 合理性があれば、オペレーショナルリスクの分類は独自の分類でよい。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。

組織・体制の整備ポイント
:リスク・コミュニケーションの充実・円滑化

- 組織・体制を整備する際のポイントは

① リスク・コミュニケーションの充実・円滑化に主眼を置くこと。

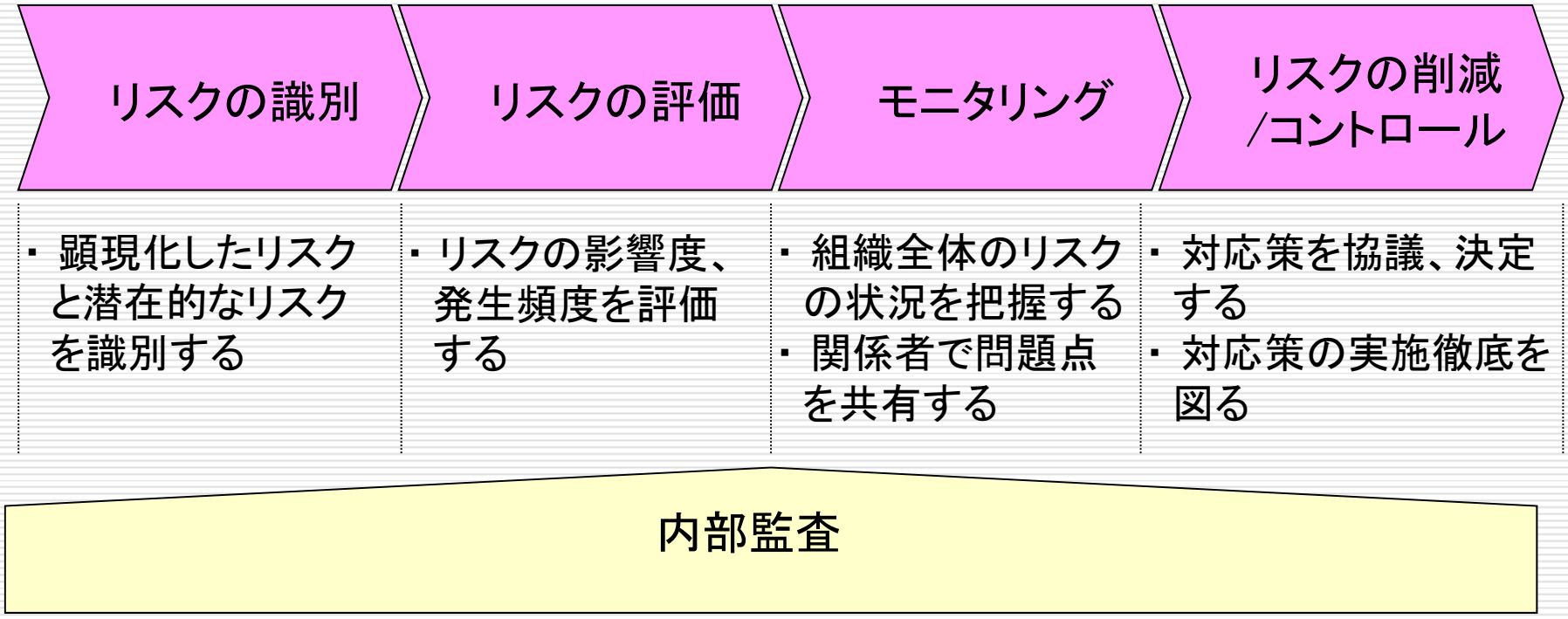
- とくに、オペレーショナルリスクは多種多様であることから、組織全体のリスクの状況を把握し、問題点を共有するためには、リスク管理の統括管理部署を設けるほか、オペレーショナルリスク管理委員会などで、リスク情報の一元的管理を図ることが重要。

② リスク・コミュニケーションを経営の意思決定に活かし、適正な対応策の実行徹底を促す体制とすること。

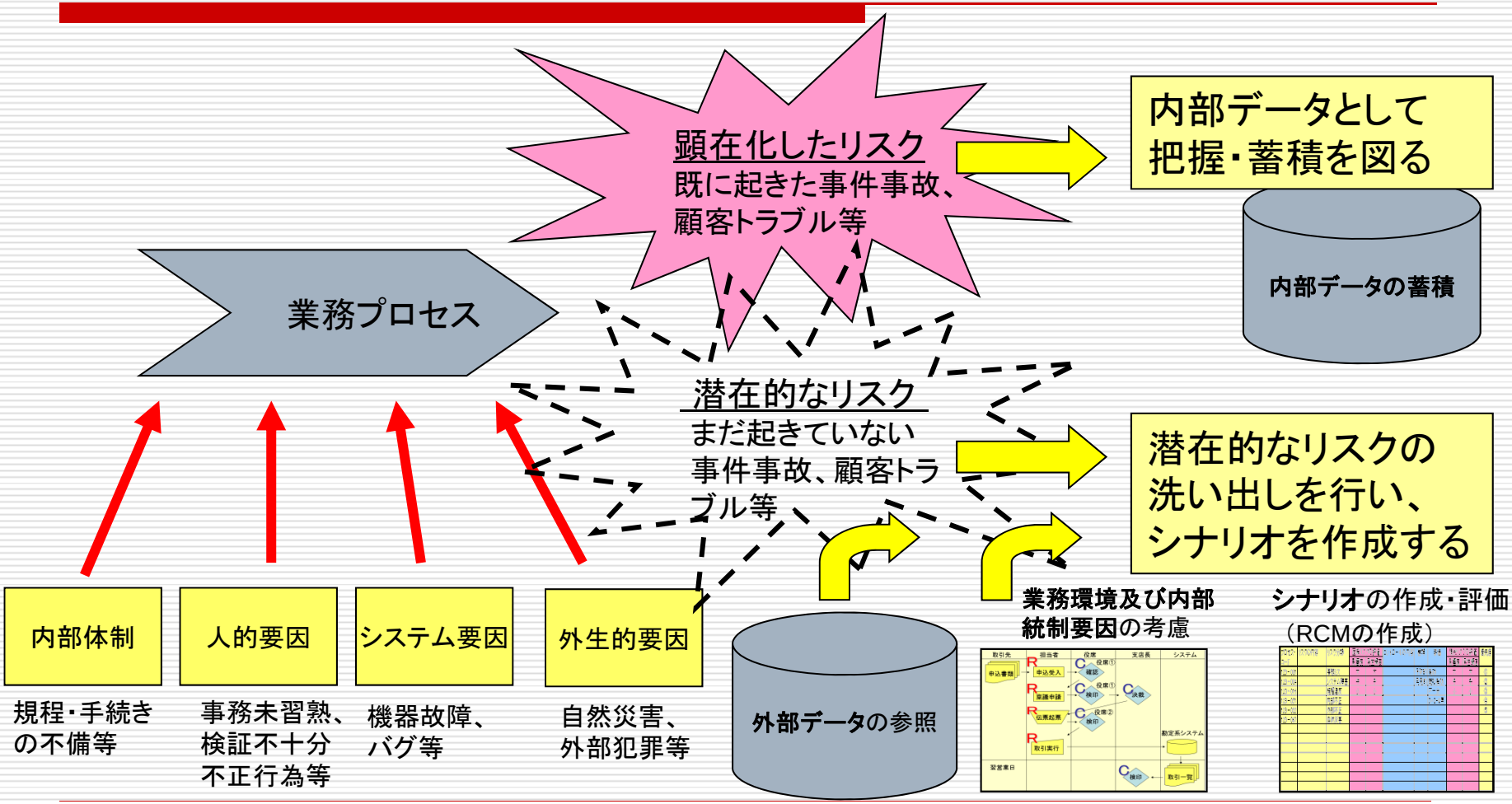
- 経営陣が対応策を協議、決定し、実行の徹底を促すためには、各リスク管理部署の実務に精通した担当者が組織横断的に連携(※)し、経営陣をチーム・サポートすることが重要。

※　WG、TF、リスク管理委員会の下部組織など

3. リスク管理の基本フレームワーク



a. リスクの識別


顕在化したリスク
既に起きた事件事故、顧客トラブル等
内部データとして把握・蓄積を図る
内部データの蓄積
業務プロセス
潜在的なリスク
まだ起きていない事件事故、顧客トラブル等
潜在的なリスクの洗い出しを行い、シナリオを作成する
内部体制
人的要因
システム要因
外生的要因
規程・手続きの不備等
事務未習熟、検証不十分 不正行為等
機器故障、バグ等
自然災害、外部犯罪等
外部データの参照
業務環境及び内部統制要因の考慮
シナリオの作成・評価
（RCMの作成）

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 バーゼル損失区分
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、各業務を所管する本部部署の管理者あるいは担当者で、現場の実務に詳しい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に内在する「重要なリスク」を識別・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

XXXXXXXXXXXXXXX

シナリオ4.

XXXXXXXXXXXXXXX

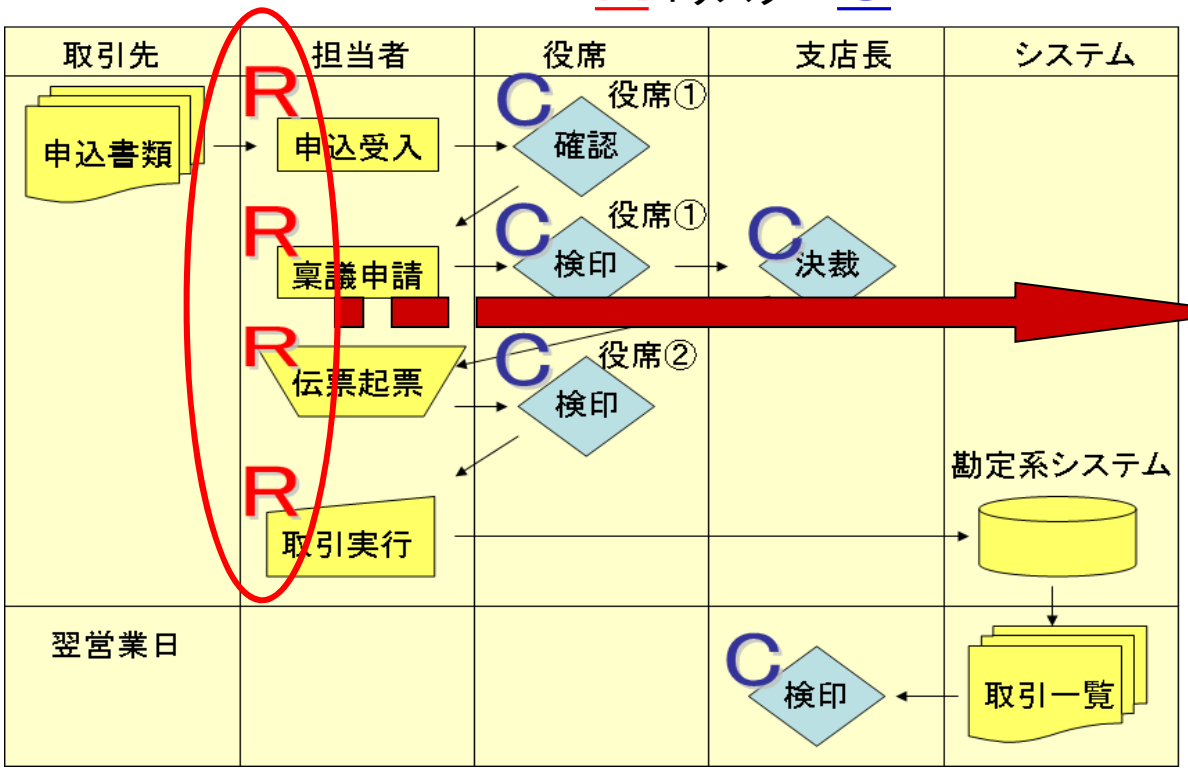
⋮

【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

XXXXXXXXXXXXXX

シナリオ4.

XXXXXXXXXXXXXX

⋮

b．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）にも注目して評価するケースもある。

リスク・コントロールマトリックス（RCM）

内部データ

シナリオ

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
		システム障害	中	中		発見的	概ね有効	中	中	②
123－016		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								

リスクの識別・評価の範囲の多様性

データ・ベースの登録件数

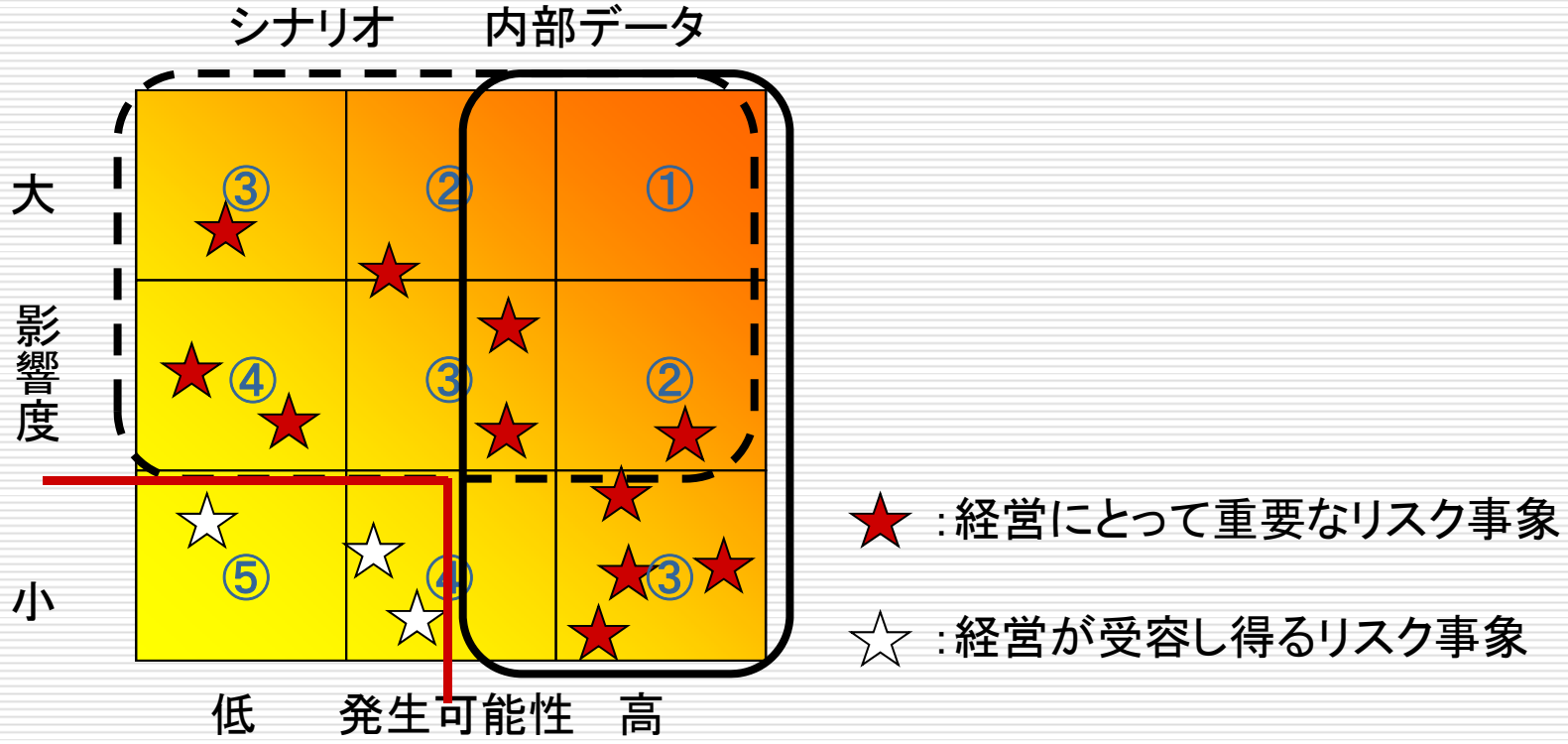
- 登録対象を一定金額以上の実損が発生した事件・事故に限定し、事務ミスなどは含めないケースであれば、月間登録件数は数件程度に止まる。
- 一方、事務ミス、顧客トラブル等も、可能な限り含めて登録対象としているケースであれば、月間登録件数は数百件に膨らむ。月間千件を上回る規模の登録がある地域金融機関も存在。

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。

経営にとって「重要なリスク」の把握

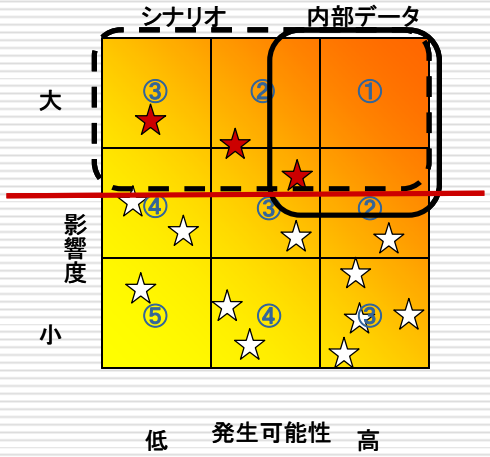
- 内部データとシナリオの組み合わせにより、経営にとって「重要なリスク」を把握する。



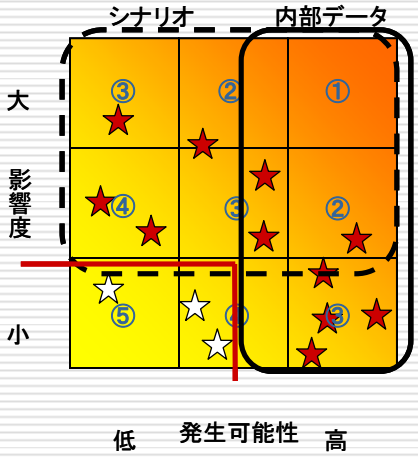
目的の明確化とデータ収集・シナリオ作成の基準

- そのためには、経営陣が主導して、オペレーショナルリスク管理の目的を明確にすることが重要。
  ⇒　内部データ収集、シナリオ作成の基準（目安）を与える。
- 目的が明確でないと、経営にとって重要なリスクは何かが分からず、形骸化しがち。

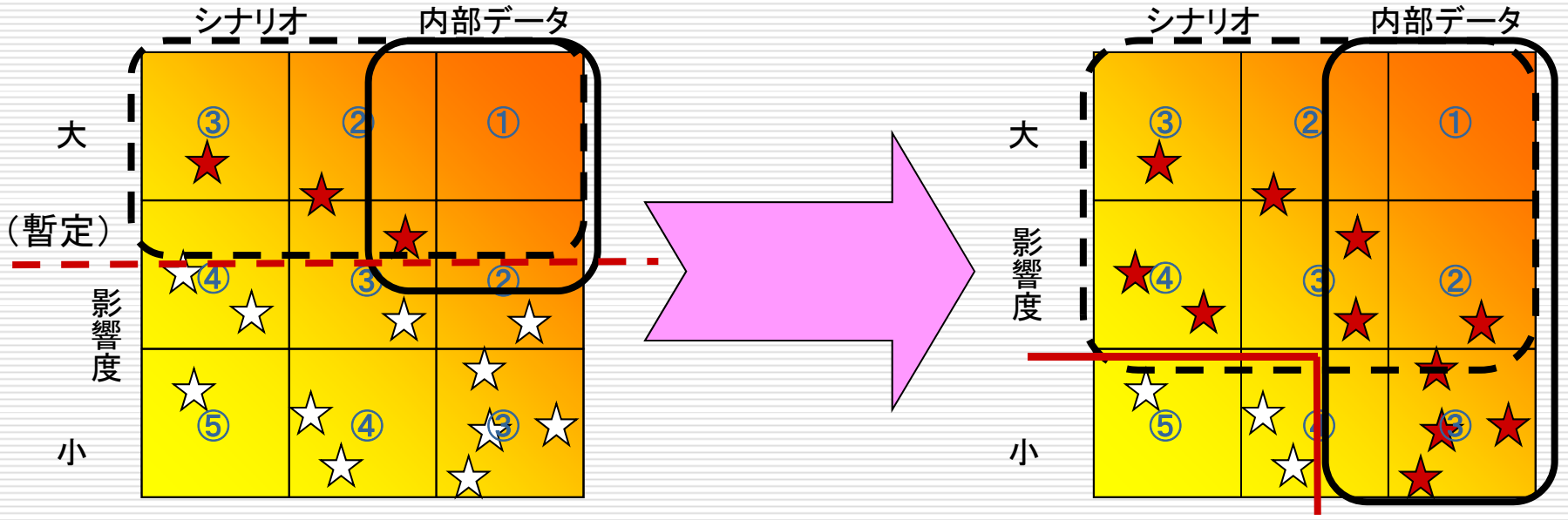
経営を揺るがす大きなリスクへの対応ができているかを確認したい。



業務プロセスの改善を図りたい。



リスクの識別・評価の対象範囲を限定してはじめ、徐々に拡大していく方法

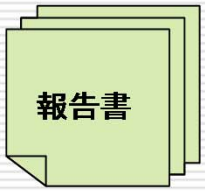


・内部データ登録基準の拡大
・シナリオ作成基準の拡大
・モニタリング体制の整備

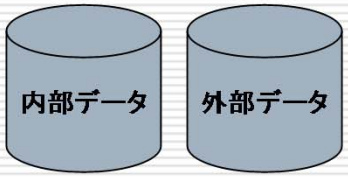
- 中小金融機関では、「シナリオの作成は難しい」と受け取られがちだが、他行事例を参考にして不正事件、重要な事務事故、システム障害などをシナリオ化することからはじめればよい。
- 日本の金融機関では、このようなセルフチェックが担当者レベルで行われてきた。CSAは、伝統的なセルフチェックを可視化し、経営陣まで繋ぐように制度化したものであると考えられる。
- データ・ベースへの登録、シナリオの作成について、対象範囲を限定してはじめ、モニタリング体制を整えながら、対象範囲を拡大していく方法もある。
- 新規業務の展開前に、CSAによる評価・検証を義務付ける金融機関も増えている。

c. モニタリング

- オペレーショナルリスクに関する情報は膨大。
- Bad News であるため、報告・登録がされなかったり、不正確なこともあり得る。



・事件・事故報告
・事務ミス報告
・苦情トラブル報告

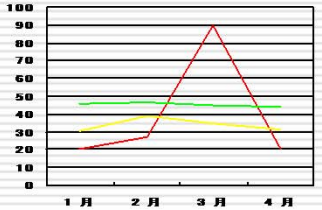


内部・外部データの分析

RCM

CSAの定期更新・随時更新

KRI



各種指標（KRI）のフォロー

- 経営としては、正確かつ迅速に情報が伝達されるよう役職員に常に働きかけると同時に内部監査等で検証を行う必要がある。
- 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たモニタリング要員の育成・確保を図ることが重要。

モニタリング情報の収集

- ”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、講話
  - 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、重要な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

モニタリング情報の収集

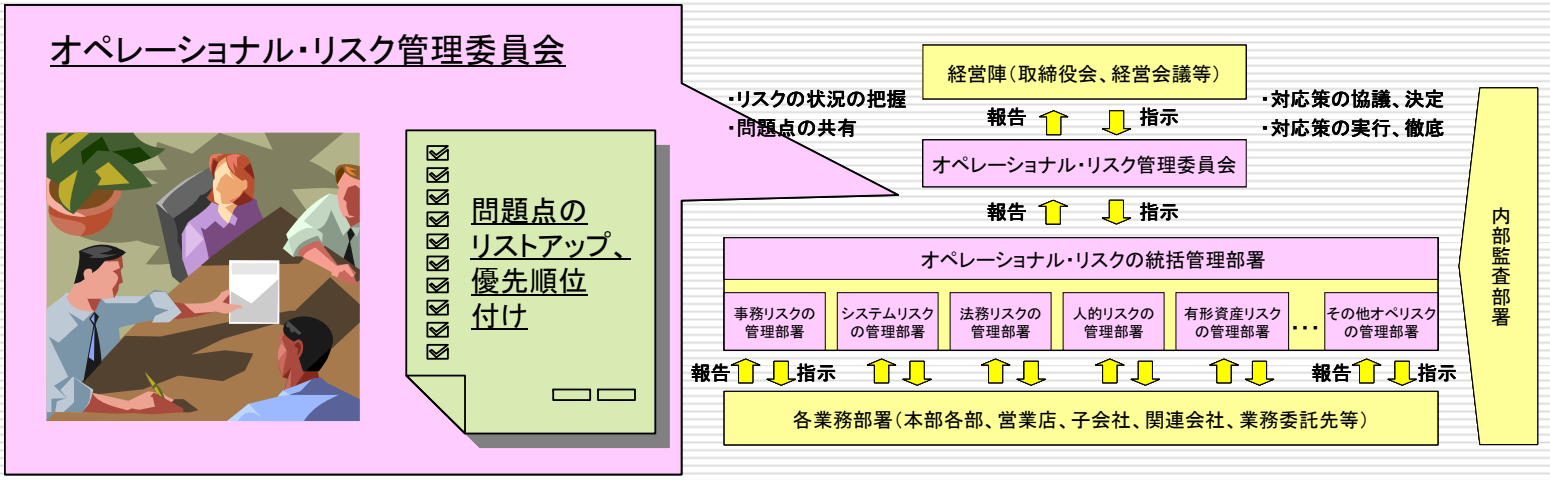
- ”Bad News”の伝達・共有へのインセンティブ
  - 問題発生の報告を受けた後、相応のスピード感をもって改善策の決定、実行に取り組み、その成果を組織内に示すことが重要。
  - 重要な事件・事故、顧客トラブル、システム障害等の発生状況、原因分析などをフィード・バックすることも、報告者の納得感や報告のインセンティブを増す。
  - ― 反対に、事件事故、事務ミスの撲滅（ゼロ）運動や、過度な報告負担などは ”Bad News” を伝達・共有する際の支障となったり、インセンティブをなくすこともあるので要注意。

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幅広く、かつ、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。

d. 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て、問題点をリストアップし、優先順位を付ける。
- それらを組織内の関係者で共有して対応策を協議、決定する。
- 決定した対応策の実行の徹底を働きかける。



リスクの重要度と対応コストの勘案

- 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、組織横断的に比較することで、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、対応の可否や優先順位を協議し、合意を得る。

（評価の目安）

  - リスクの重要度との比較で、対応コストが過大になっていないか（多額のシステム投資をするほどの案件か）。
  - 対応コストを抑え過ぎているため、効果が期待できないのではないか（注意喚起に止めてよい案件か）。

e. 組織文化の醸成

- 組織文化がリスク･コミュニケーションを支える。

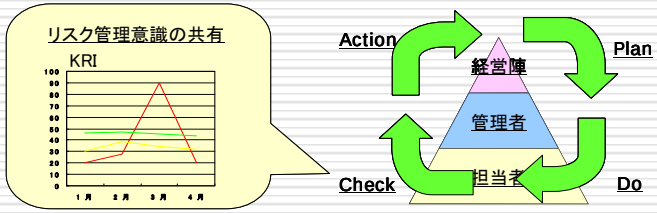
（組織文化を醸成する方策）

- 経営陣からの働き掛け
- 営業店CSAの実施
- KRI指標の共有
- 3点セットの共有
- 研修の実施

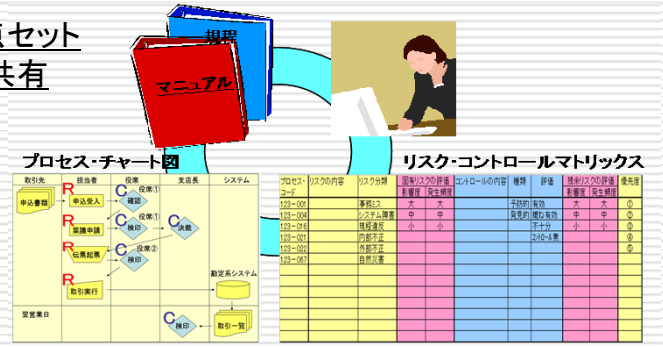
営業店CSA

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		

KRI指標の共有

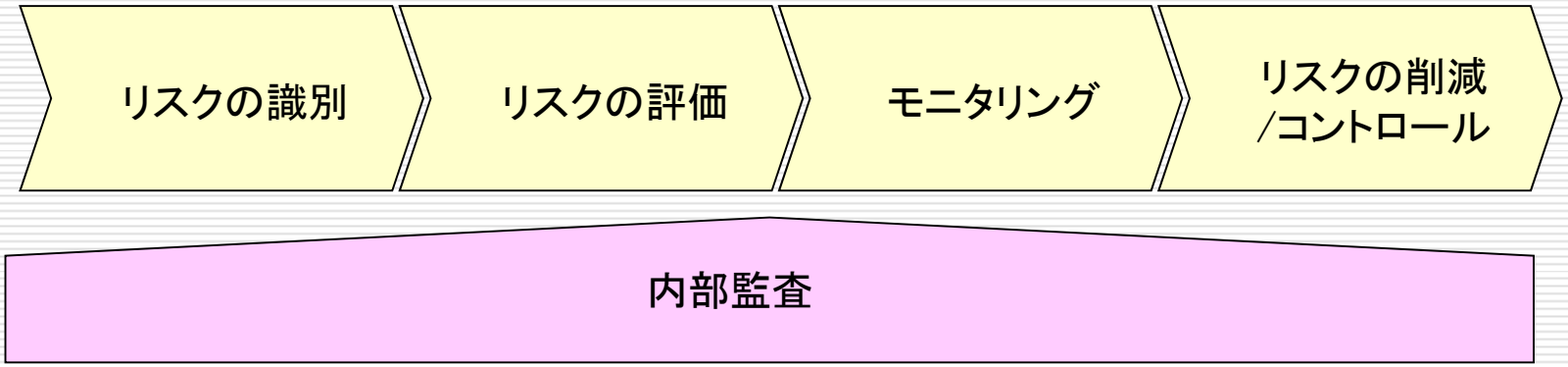


3点セットの共有



f. 内部監査による検証

- 内部監査では、オペレーショナルリスク管理の組織・体制が適切に構築されているか、また、リスクの識別、評価、モニタリング、削減/コントロールという 基本フレームワークの各段階で、効果的な措置が講じられているか、を検証する。
- 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。



検証のポイント

（組織・体制）

- ✓ オペレーショナルリスクをカテゴライズして、それぞれに管理部署を定めているか。
- ✓ 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置しているか。
- ✓ オペレーショナルリスクの統括管理部署と各リスク管理部署が連携して、モニタリングと経営判断のサポートを行っているか。
- ✓ オペレーショナルリスクの統括管理部署と各リスク管理部署は、フロント部署に対する牽制機能を発揮しているか。

検証のポイント

（リスクの識別・評価）

- ✓ 顕現化したリスクだけでなく、潜在的なリスクも含め、重要なオペレーショナルリスクを識別・評価しているか。
- ✓ オペレーショナルリスクの影響度、発生可能性を評価する際、その客観性を高める措置を講じているか。

（モニタリング）

- ✓ オペレーショナルリスクに関する重要情報が、迅速かつ正確に、組織内で伝達、共有されているか。
- ✓ モニタリング要員は膨大な情報を適切に収集、整理、分析する実務知識、能力があり、組織全体のオペレーショナル・リスクの状況を的確に把握しているか。

検証のポイント

（リスクの削減/コントロール）

- ✓ リスク事象の詳細や発生原因を十分に分析し、再発の防止や抑制に繋がる適切なコントロールを設計・導入しているか。
- ✓ コントロールの導入の可否、優先順位を決める際、可能な限り費用対効果を勘案して、組織的に協議し、合意を得ているか。
- ✓ コントロールの徹底を図るため、経営陣が率先して規律重視の組織文化の醸成に努めているか。

4. データ・コンソーシアムの活用可能性

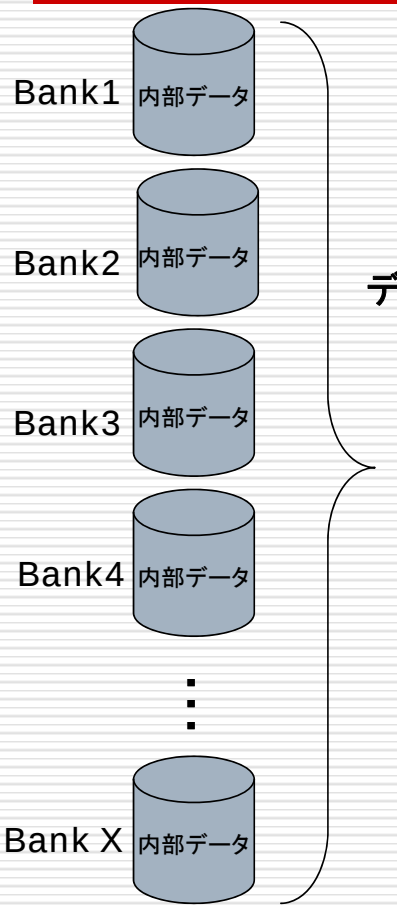
- 地域金融機関 数行が、自主的にデータ交換、シナリオ交換を開始。

  - 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

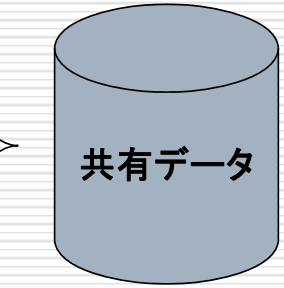
      （主要登録項目のほか、銀行情報・個人情報をマスキングして概要を記載）

- 上記取り組みを契機にして、データ・コンソーシアムが設立された。

データ・コンソーシアムの活用可能性

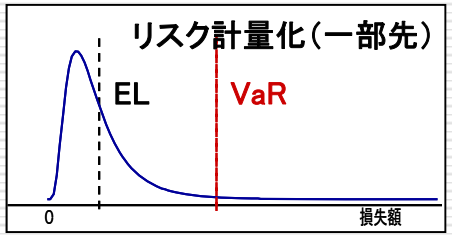


データ・コンソーシアム

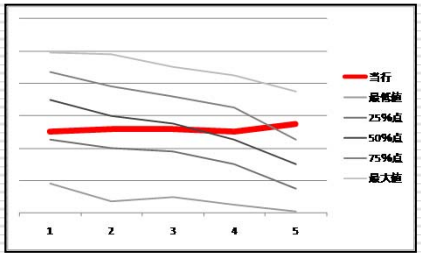


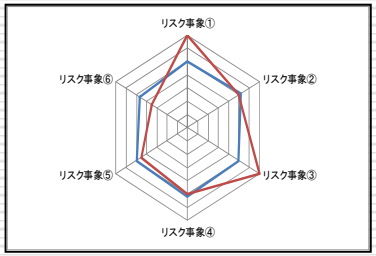
①重要なリスク事象の把握・評価： 網羅性、客観性の向上

カテゴリー	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				
	為替事故（誤送信・処理遅延等）	XXXX XXXX	XX件	XXX 円	○（有）
		XXXX XXXX	XX件	XXX 円	×（無）
		XXXX XXXX	XX件	XXX 円	×（無）
		XXXX XXXX	XX件	XXX 円	×（無）
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				

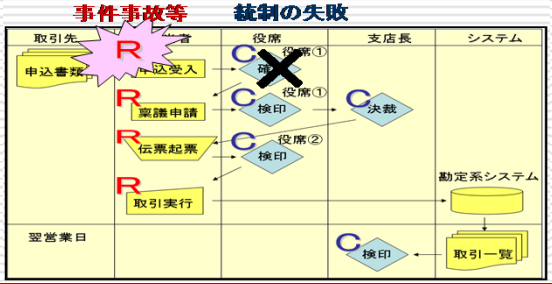


②データ分析の高度化： リスクプロファイル、強み・弱みの把握



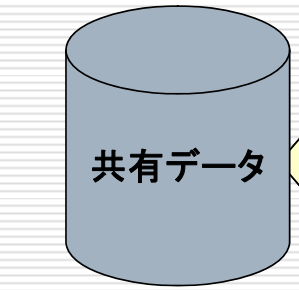


③業務プロセスの検証： 問題点の洗い出しと対応策の検討



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。



データ・コンソーシアム

重要なリスク事象に関する情報

カテゴリー	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				
	為替事故（誤送信・処理遅延等）	XXXX XXXX	XX件	XXX 円	○（有）
		XXXX XXXX	XX件	XXX 円	×（無）
		XXXX XXXX	XX件	XXX 円	×（無）
		XXXX XXXX	XX件	XXX 円	×（無）
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				

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

④ 最近、新たに発生し始めたリスク事象

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金融機関がデータ・コンソーシアムに参加して、10年間に1回だけ発生したリスク事象があれば、その発生可能性について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。

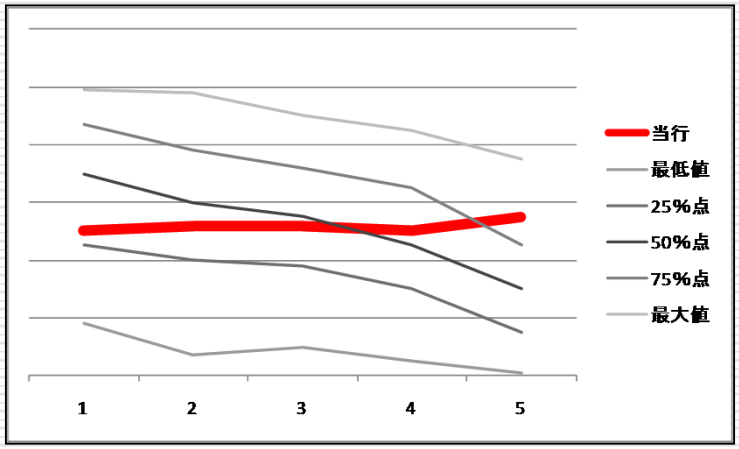
データ・コンソーシアムの活用事例

- 内部データベースの構築・更改にあたり、共同データベースの管理ノウハウを吸収するために、データコンソーシアムに参加する金融機関が増加。
- これまで潜在的なリスク事象に係るシナリオを作成したことのない金融機関に対して、データ・コンソーシアムが「共通シナリオ」の提供サービスを開始。

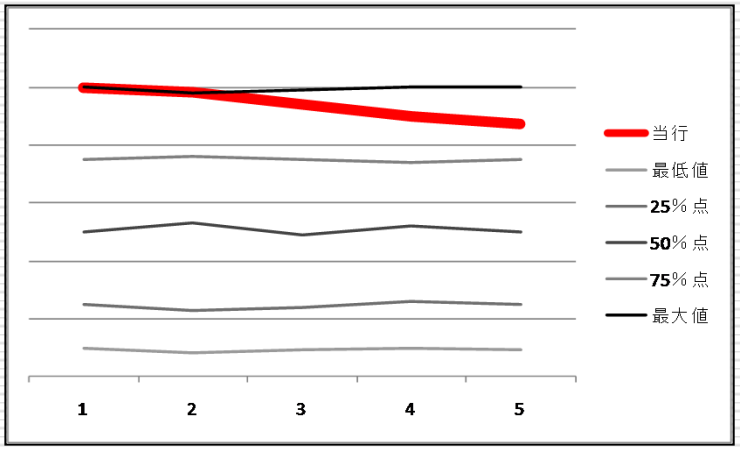
② データ分析の高度化

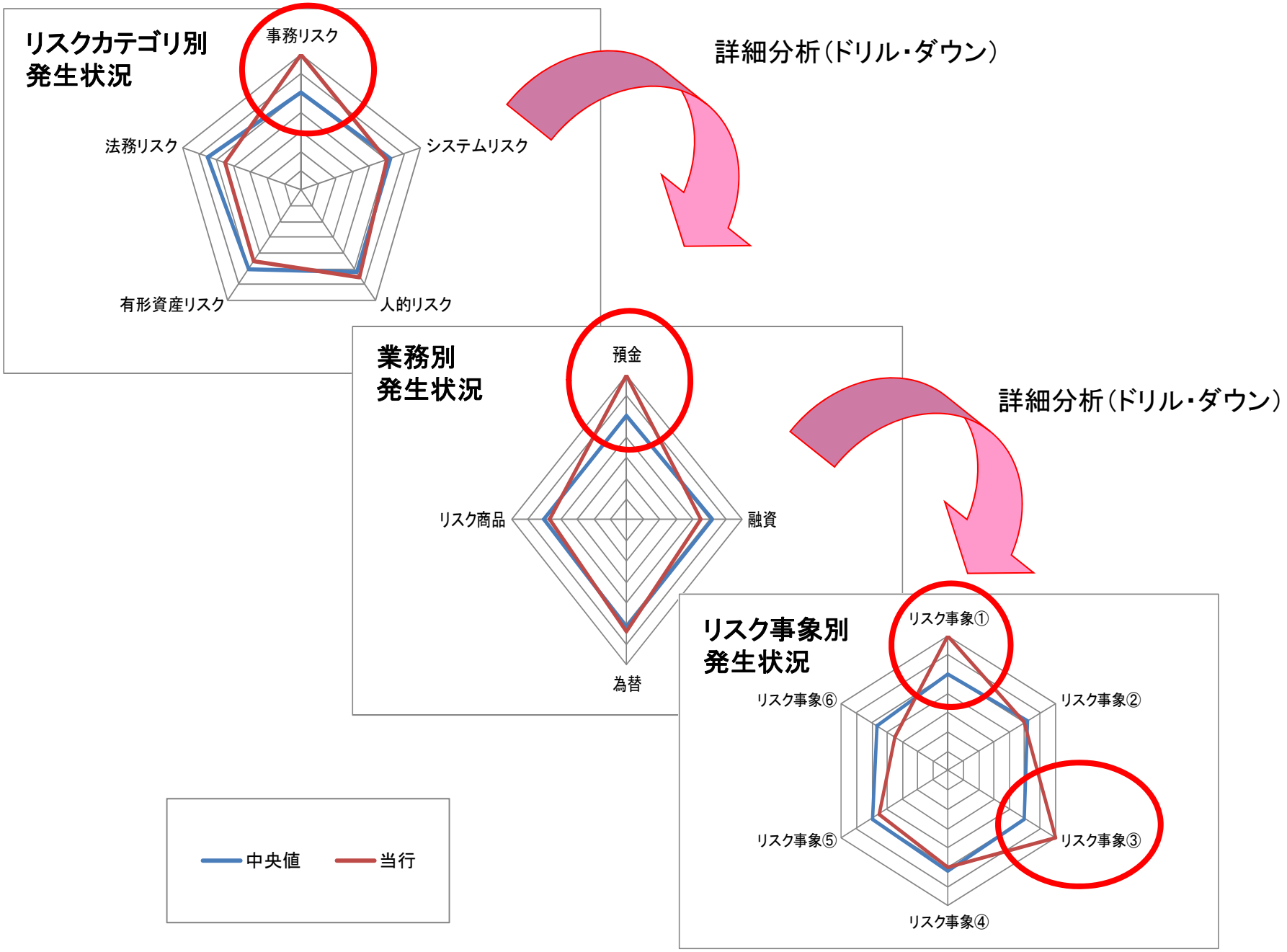
- 多くの金融機関のデータが集まれば、集計値・傾向値と比較することにより、自らのリスクプロファイルの特徴や統制面の「強み・弱み」などを把握・分析することができる。

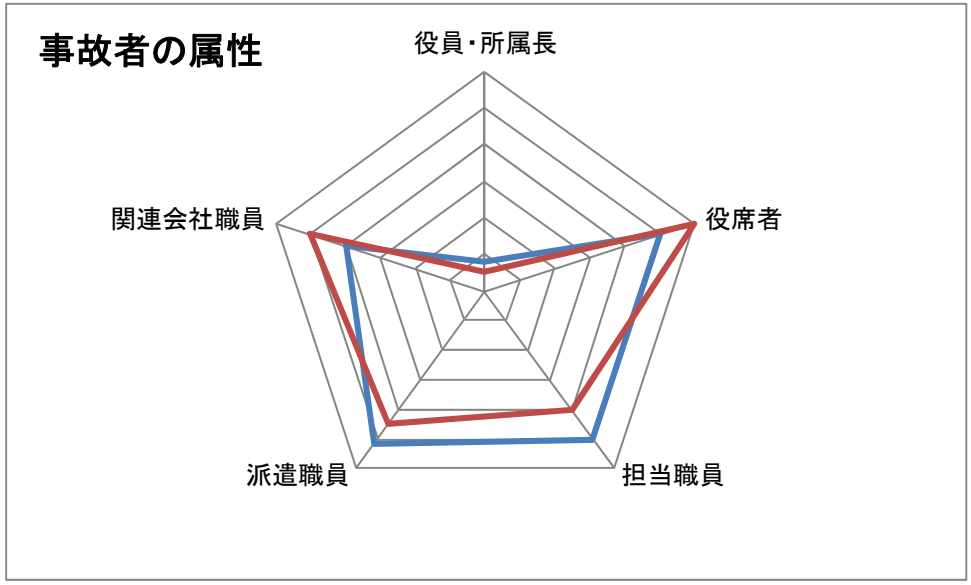
（例）リスク事象①の発生状況



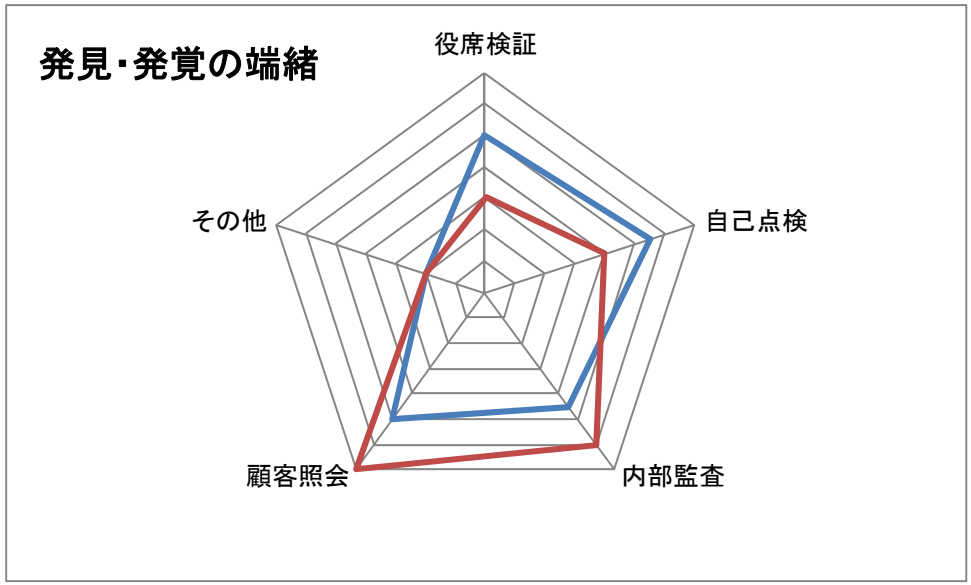
（例）リスク事象②の発生状況




リスクカテゴリ別
発生状況
事務リスク
システムリスク
人的リスク
有形資産リスク
法務リスク
詳細分析（ドリル・ダウン）
業務別
発生状況
預金
融資
為替
リスク商品
詳細分析（ドリル・ダウン）
リスク事象別
発生状況
リスク事象①
リスク事象②
リスク事象③
リスク事象④
リスク事象⑤
リスク事象⑥
中央値
当行



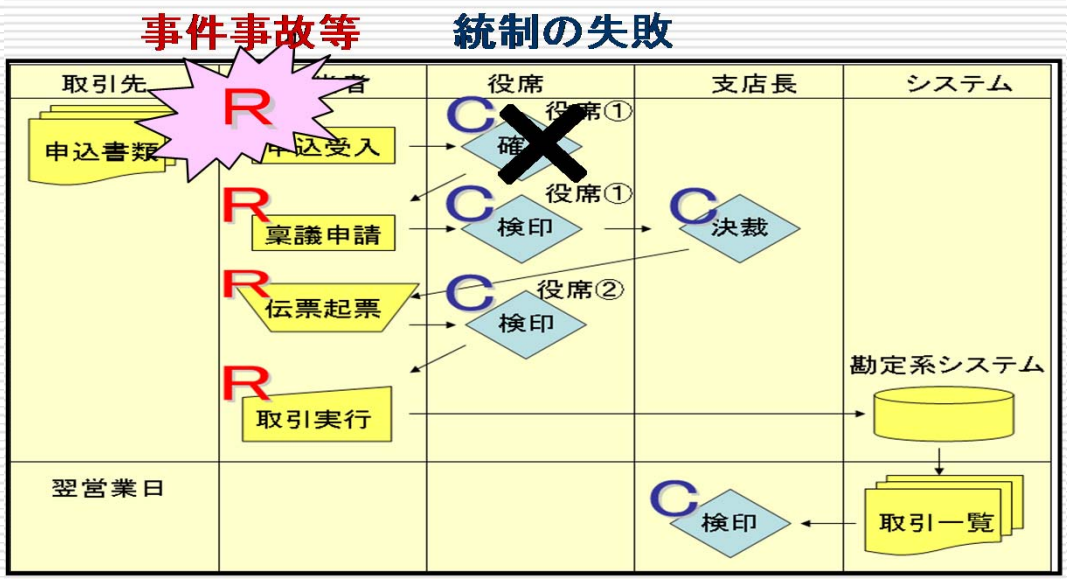
事故者としては、担当者、派遣職員が少ない一方、役席者、関連職員が多い。



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。

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。

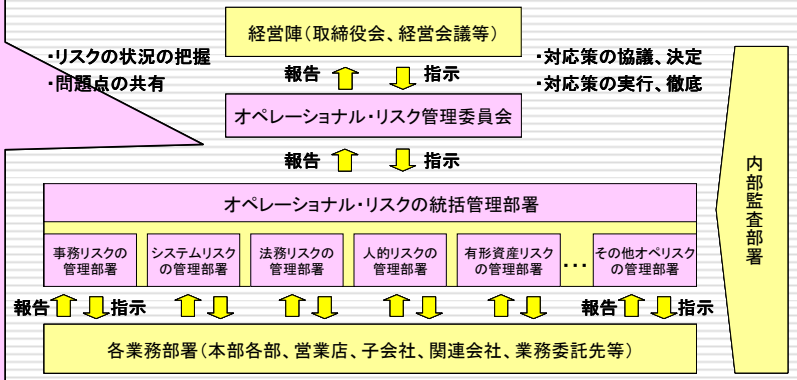


リスク事象の事例研究とリスク・コミュニケーション

- 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！



留意点

① 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る。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。

② データ・カストディアンの機能度

— データを標準化し、共通のリスク事象区分に仕分けたり、共通のシナリオの提供を行うデータ・カストディアンの機能度がデータベースの価値を左右する。

③ 自行サイドのモニタリング要員の確保、体制整備

— 提供された他行データを分析し、自行のリスク管理に活用し得るモニタリング要員の確保、体制整備が必要となる。

④ 参加コストと活用方法の検討

— コンソーシアムへの参加コストと、自ら他行事例を集めるコストを比較したり、データ活用方法とその効果を予め検討する必要がある。

- 本資料に関する照会先

  日本銀行金融機構局金融高度化センター

  企画役　碓井茂樹　CIA,CCSA,CFSA

  Tel　03(3277)1886　E-mail shigeki.usui@boj.or.jp

-

- 本資料に掲載されている情報の正確性については万全を期しておりますが、日本銀行は、利用者が本資料の情報を用いて行う一切の行為について、何ら責任を負うものではありません。