公認内部監査人(CIA)
Part I／第6回

※アビタスCIA本講座講義資料のため、MUFG CIA受験対策講座の実施回と異なります。

6-12 リスク・マネジメントの評価に用いるツール

リスク・マネジメントの評価に用いるツール

内部監査人はリスク・マネジメント・プロセスの有効性を評価するため、リスク・マネジメントに用いるツールについて理解する必要がある。

論点　リスク・マネジメントの評価に用いるツール

リスク・マネジメントのための代表的なツールは以下の通り。

内部統制質問書	内部統制質問書は、活動やプロセスが分析され、適切な統制が存在することが確認された後に作成される。“はい”“いいえ”の直接的な回答を求めることによって、期待される手続きが遵守されているかを確認する。統制が継続して存在することを確認し、リスクの評価を可能にすることを意図している。
業務記述書 （ナラティブ）	業務記述書では個々の業務における作業内容や手順を記載する。作業の概要、管理方針や職務分掌等を含む。

内部統制文書化の3点セット

フローチャート	フローチャートは、業務の有効性と統制について分析する手法である。視覚的でわかりやすく、通常インターナル・コントロールの重要な部分を見落としにくい。一度作成すれば、レビューの上更新を重ねることによって、複数のフローチャートを比較し分析することが可能になる。
リスク・コントロール・マトリクス（RCM）	リスク・コントロール・マトリクスでは、各プロセスをリスクベースに分類し、リスクの内容、対応する統制、及び該当するアサーション等を記述する。

3点セット：

各部門が作成し、内部監査人が有効性を評価する

マトリクス分析	マトリクス分析では、各リスクはそれぞれ適切な統制で補填されているということを確かめるために、統制とリスクを一致させる。統制マトリクスによって、統制が一つ以上のリスクを補填していることを認識することも可能である。
リスクマップ	リスクマップに画一的なフォーマットは存在しないが、典型的なリスクマップは、リスクの影響度を縦軸に、その発生可能性を横軸にとって、リスクを俯瞰的に描写することで、リスクに関する情報の理解を容易にするものである。

Key Point：

a) 内部統制質問書の例

Yes/No Questions，内部監査部門が作成

質問	回答		内部監査人記入欄		
	はい	いいえ	備考	方法	実施担当者
1. 文書化された購買方針が存在しているか？	✓			書面を確認	監査太郎
2. 購入申請書は権限のある者によって承認されているか？	✓		購入申請書は購入希望部門の部門長の承認が必要になる。	書面を確認	監査太郎
3. 物品は承認された業者から購入されているか？	✓			質問	監査花子

内部統制質問書は、最初のリスク評価が実施された後、更なる評価を実施する際のチェックリストとして使われる。従って、内部統制質問書の内容は、その時々の企業の目的に合致していなければならず、業務上の変更が生じた場合は質問書の内容も更新していかなければならない。

原則：予備調査の段階で行う

例外：現場作業の段階で行う

b) 業務記述書の例

以下の例は、販売プロセスにおける取引先申請の承認というコントロール・ポイント(統制点)における業務記述書である。

I. 会社の概要
   1. 業種
   2. 組織体制
      (組織図)

II. 主要な業務プロセス
   1. 販売プロセス

会社名	CIA 株式会社
担当部門	営業・販売本部、物流センター、経理部
プロセス	販売
プロセス・オーナー	営業統括部長：営業太郎 物流センター長：物流花子 経理部長：経理次郎
関連勘定科目	現金預金、売掛金、売上
関連情報システム	与信管理システム、販売管理システム、得意先顧客マスター、販売単価マスター
関連諸規程	職務分掌規程、販売管理規程、在庫管理マニュアル、経理規程、情報システムマニュアル
作成者： 作成日：	

1-1: 取引先申請

販売プロセスにおける営業部による取引先申請の承認では、以下の点を確認する。

1） 営業部担当者は、販売管理規程に基づいて新規取引先の信用調査を実施した上で基本契約を締結している。

2） 営業統括部長は新規取引先の承認においては、販売管理規程に基づいて、取引先申請書に記載された信用調査の結果と与信限度額を査閲し、取引先申請書に押印している。営業担当者は、承認済取引先申請書を経理部に回付し、マスター登録を依頼する。

3） 経理部長は、取引先申請書の記入漏れがないかを確認し、押印する。経理担当者は承認済取引先申請書に基づき、得意先顧客マスター、与信管理システム、及び販売単価マスターに必要な情報を入力する。

⋮

1-2：受注
1-3：出荷
1-4：売上計上

販売プロセスにおける売上計上においては、以下の点を確認する。
1） 出荷処理されたデータは夜間バッチ処理により売上データに変換され、販売管理システムに伝送される。出荷が完了した受注については受注データが自動的に消しこまれる。
2） 営業経理は前日の売上報告書を販売管理システムから出力し、出荷報告書との照合を行う。
3） 営業部門の責任者は、受注データの消しこみが適切に行われているかどうかを確認するため、定期的に注文残リストを査閲している。

1-5：請求
1-6：債権管理(回収)
⋮

業務記述書(ナラティブ)

社内の各業務プロセスの一連の流れを、

文章によって表現したもの。

Key Point

利点：プロセスの流れがすべて分かる

欠点：情報過多

一連の業務の流れを視覚的に示したもの

c) フローチャートの例

各コントロール・ポイントには、リスク及び対応するコントロールを記載する。この例では、営業部の取引先申請書の承認において、次ページのRCMに記載されているリスク番号R1、R2のリスクが考えられ、対応する統制として、統制番号C1、C2、C3、C6、及びC8がある。

R1は、例えば営業担当者が独断で取引先をマスター登録してしまった場合に現実化するリスクである。このような営業担当者の行為を発生させないために、C1、C2、C3に記載されている統制が必要になる。

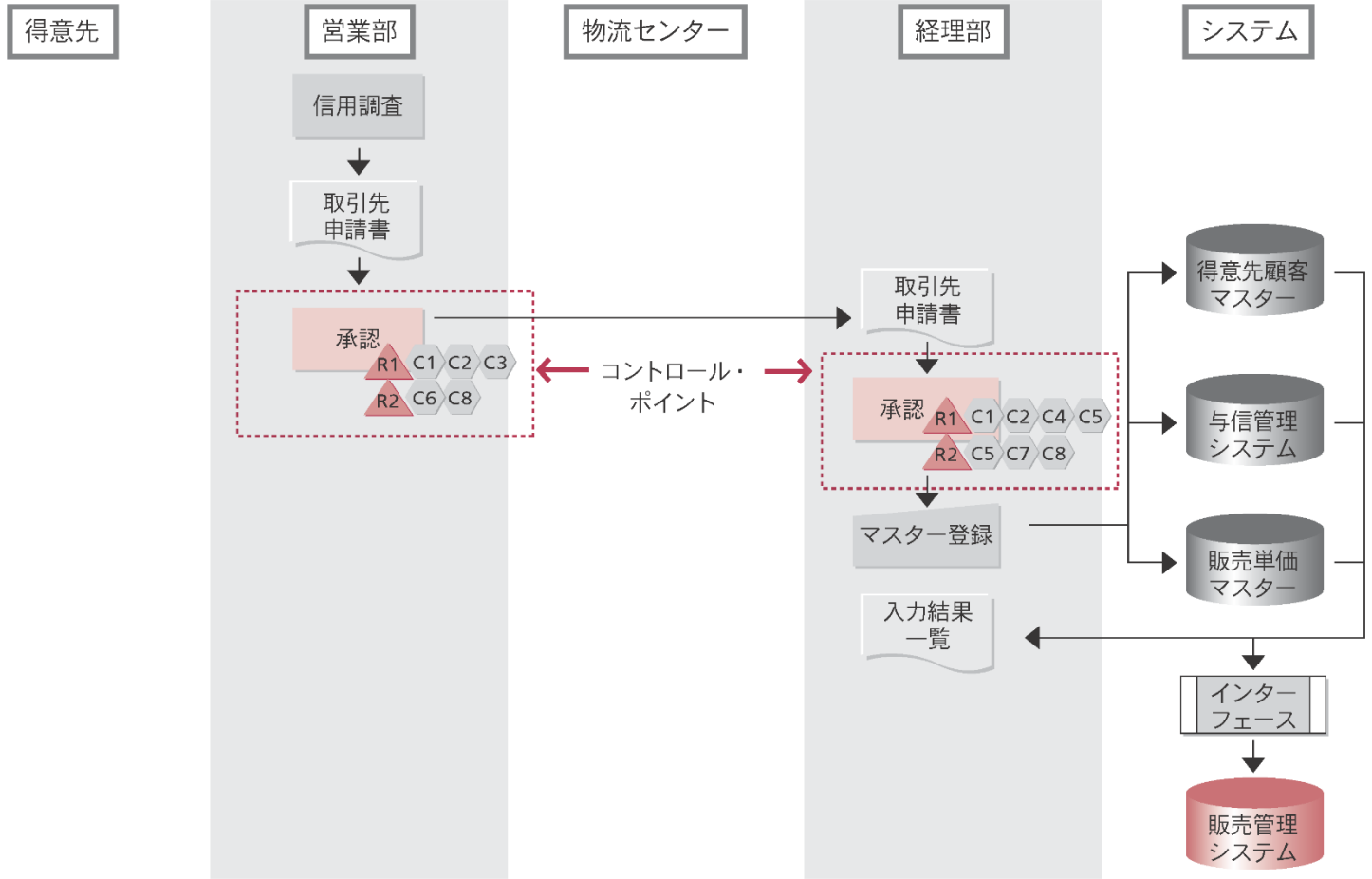
Key Point

利点：ビジュアライズ化されているため分かり易い

欠点：ITシステムを多用すると作成が困難

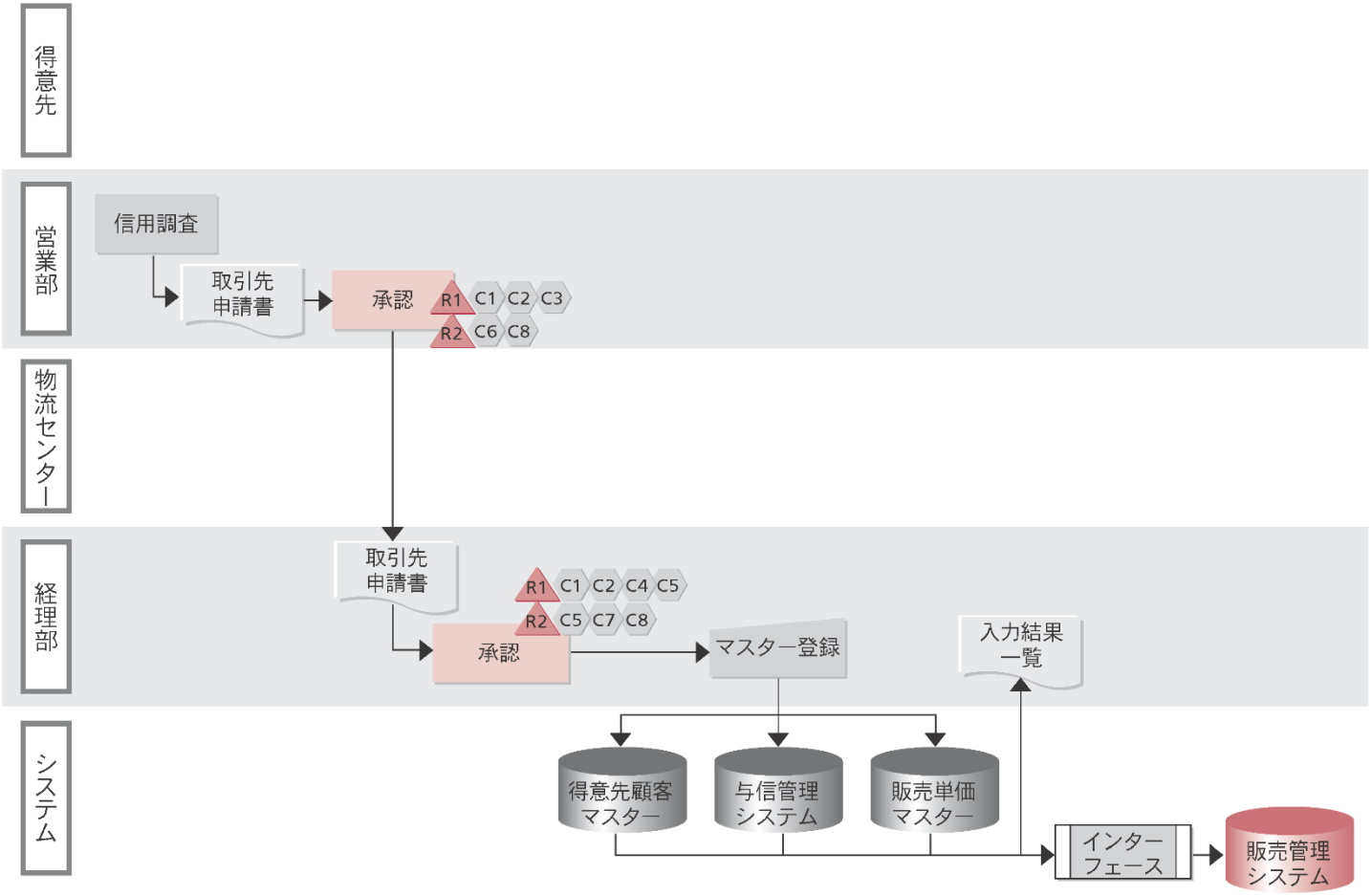
前提： 時間が縦に流れることを優先した表現

〈縦書きフローチャートの例〉



前提： 部門別の職務分掌を優先した表現

〈横書きフローチャートの例〉



Key Point

縦書フローチャートと横書フローチャートの特徴

縦書フローチャート	横書フローチャート
• 縦に時間が流れるフローチャート • 部門単位を重視した記載方法 • 説明文を多く書き込める • ページ数は多くなる	• 横に時間が流れるフローチャート • 時間や処理の流れを重視した記載方法 • 説明文を書き込むスペースが少ない • ページ数は少なくなる

- **不適切な職務分離を明確に示す**

d) リスク・コントロール・マトリクス(RCM)の例

以下は、販売プロセスにおけるRCMの例である。

サブプロセス	リスク		統制				
	番号	内容	番号	内容	種類	形式	
取引先申請・承認	R1	販売単価マスター、得意先顧客マスターに正確な情報が入力されない。	C1	取引先申請、マスター登録の手続きは販売管理規程内に文書化されている。	予防的	マニュアル	
			C2	マスター登録と受注入力の担当部署の分離は職務分掌規程に文書化されている。	予防的	マニュアル	
			C3	営業統括部長は取引先申請書への押印によって、申請を承認している。	予防的	マニュアル	
			C4	経理部長は取引先申請書への押印によって、申請を承認している。	予防的	マニュアル	
	R2	販売単価マスター、得意先顧客マスターの変更、更新が適切に行われない。	C5	経理部長はアクセス権限変更依頼書に押印して、各マスターへのアクセス権限変更を承認している。	予防的	マニュアル	
			C6	各マスターへのアクセス権限は情報システムマニュアルに基づいて入力画面上のパスワード入力で管理されている。	予防的	IT	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

		証跡		アサーション				
実施頻度	実施者	名称	保管場所	実在性・発生	網羅性	権利・義務	評価・配賦	表示・開示
継続的		販売管理規程		○		○		
継続的		職務分掌規程		○		○		
随時	営業統括部長	取引先申請書	経理部	○		○		
随時	経理部長	取引先申請書	経理部	○		○		
随時	経理部長	アクセス権限変更依頼書	経理部	○		○		
随時		情報システムマニュアル	システム管理部	○		○		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

RCM

想定されるリスク、対応するIC活動、

ICの種類等を一覧表にしたもの

e）　マトリクス分析の例

	統制Ａ	統制Ｂ	統制Ｃ
リスク１	主		利用可能
リスク２	補	主	利用可能
リスク３			主

Source:"Sawyer's Internal Auditing"

- 統制Ａがリスク１を補填するために設計されたとする。統制Ａがリスク１に対する主たる防御策であるため、この統制の保証レベルは“第一義的（主要）”となる。
- 同様に、リスク２は、第一義的に統制Ｂによって補填されるが、統制Ａもリスク２を一定の範囲で補填する。ただ、保証レベルは“補助的”となる。
- 同様にリスク３についても、第一義的には統制Ｃによって補填される。ただ、統制Ｃは、リスク１、２についても利用可能である。利用可能という保証レベルは、その統制のみではリスクを補填することは出来ないが、“危険な兆候”として調査を促す。

統制マトリクスをコンピュータに保存されているデータへの侵入リスクとアクセス統制の具体例で説明する。

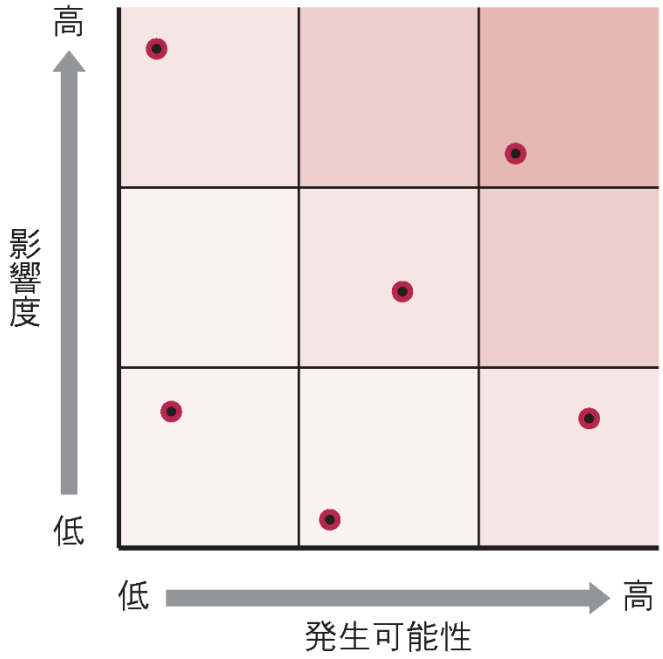
コンピュータに保存されているデータへの侵入リスクとアクセスコントロールの例。

リスク	コントロール（統制）
1. 無許可の従業員によるデータへのアクセス	A. データへのアクセスのためにIDとパスワードを要求する
2. 外部の無許可の者による企業のデータへのアクセス	B. 許可を得た外部者からリクエストがあった時のみ接続し、各利用終了時にモデムの接続を遮断する
3. 企業内外を問わず、無許可の者がデータへのアクセスを試み、将来的に侵入が成功する可能性	C. 無許可の者がデータへのアクセスを試みたという記録をセキュリティー・システムで日々出力し検証する

リスク２の場合、第一義的な統制はコンピュータへの接続そのものを切断するＢであるが、仮に各利用終了時にモデムの接続が切断されなかった場合、データへのアクセスに対し、統制Ａが補助的に補填する。又、外部の侵入者が複数回アクセスを試みている場合は、統制Ｃにより、セキュリティ担当者に注意を喚起することが可能になる。

f) リスクマップの例

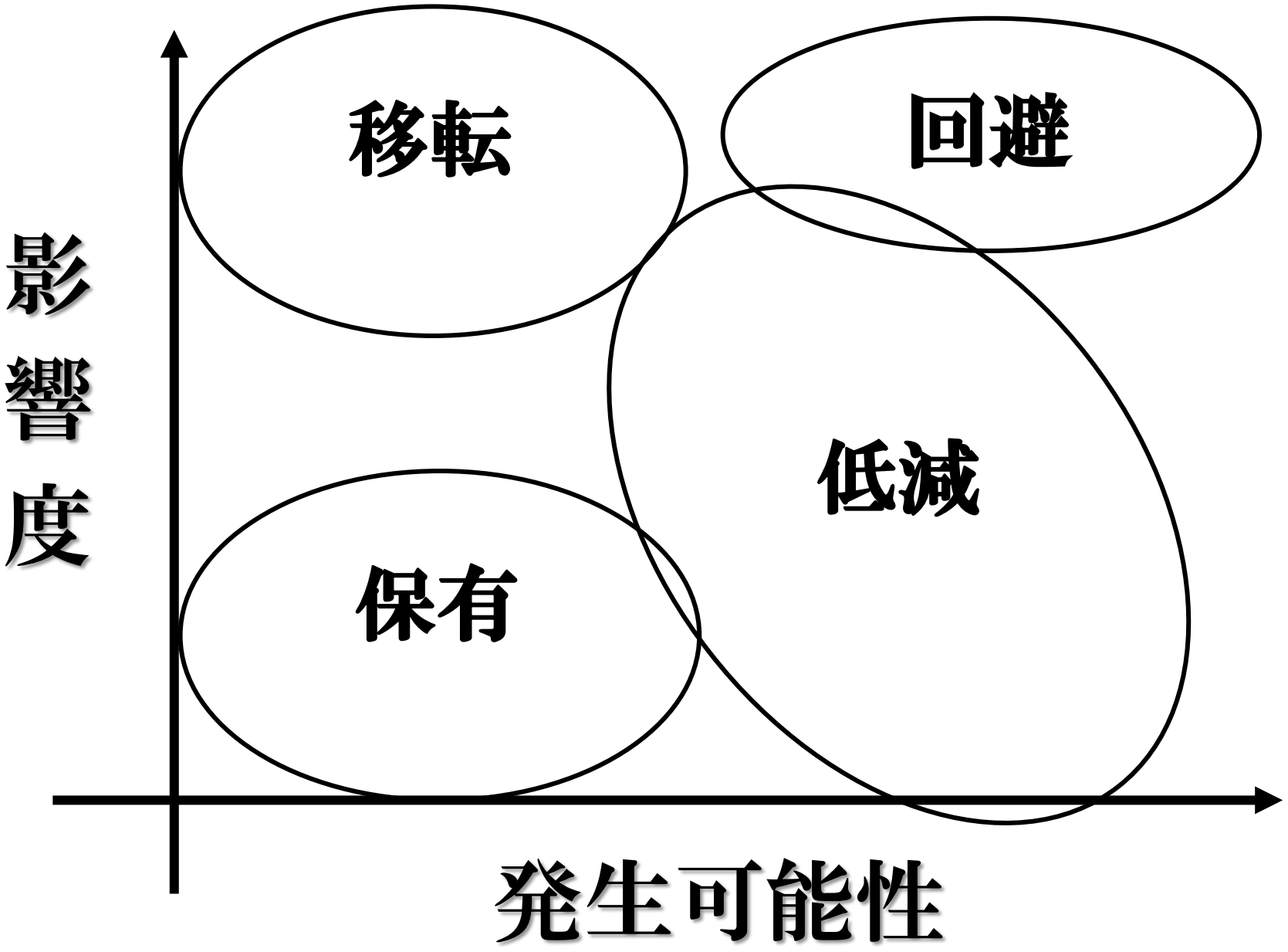
リスク分析の結果として、作成されることの多いアウトプットの１つであり、リスクの発生頻度と影響度を容易に理解することを可能とする。その結果、リスク対応の選択肢の選択も検討しやすくなる。



リスクマップ

リスクを2つの評価軸で評価した結果を、

視覚的に確認するためのツール


移転
回避
低減
保有
影響度
発生可能性

本日の論点

- ISO 31000
- RMに用いるツール
- 事業継続リスクのマネジメント
- 内部監査部門のリスク

Chapter 6

◎ 1, 3, 7, 8,

9, 12

Key Point

ヒートマップの限界はなにか？

A: 財務数値の項目でしか作成できない

B: 発生可能性と影響額のどちらが重要かの観点に欠けることがある

C: リスクマップがないとできない

D: 定性的評価ではできない