リスク評価手法の内部監査での 25 の活用事例
～内部監査での活用方法・改善提言のための確認事項～

一般社団法人　日本内部監査協会
ＣＩＡフォーラム No.a3　ＥＲＭ研究会（第９期）
２０１６年１１月

「ＣＩＡフォーラム」は、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、一般社団法人日本内部監査協会の組織上の研究会の一つです。各ＣＩＡフォーラム研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信しています。

本報告書は、本研究会（CIA フォーラム No.3a　ERM 研究会）が、その活動成果として取りまとめたものです。本報告書に記載された事例は、全て本研究会メンバーが会合・合宿等で合議して作成したものであり、研究会メンバーが所属する個別企業等の事例ではありません。報告書に記載された意見・コメント・その他の記載も同様に、全て本研究会としての見解であり、メンバー、およびメンバーが属する組織の見解ではありません。また、協会の見解を代表するものではありません。

目　次

Ⅰ．はじめに

１．リスク評価の重要性と課題

（１）有効なリスク評価

・リスクを抽出し、リスク対応の優先順位付けを行なうことは、リスクマネジメントの基本です。
・リスク対応について、限られたリソース（人員・時間・予算等）を、どのリスクにどの程度投入すべきかの判断が、実務上は常に問題になります。
・リスクを把握し、対応の優先順位付けをし、重点的にリソースを投入すべきリスク、ある程度のリソース投入で十分なリスク、リソース投入が不要なリスク等の区分をつけて、一律ではなくメリハリの効いたリソース投入を行うことが、有効かつ効率的なリスクマネジメントにつながります。

（２）課　題

・リスク評価は、対応するリスクを優先順位付けして絞り込むためのリスクアプローチの手法として**全社的リスクマネジメント（ＥＲＭ）の主要な構成要素**であると共に、**内部監査でリスクアプローチの手法を用いて監査対象を絞り込むための前提**です。そのため、リスク評価の手法は、リスクマネジメント、内部監査の双方にとって重要です。
・しかしながら、リスク評価の手法は様々な報告書や書籍で詳細に紹介されていますが、内部監査の実務で活用しようとする場合には、なかなかフィットしたものが見つけにくいのが現状です。その理由の一つは、記載が抽象的であり、イメージが掴みにくいことがあると我々は考えました。
・そこで、本研究会ではリスク評価手法の**内部監査への活用方法**やリスクアプローチへの活用をはじめとする**具体的な内部監査への活用事例**を研究しました。
・作成に当たっては、最初にリスク評価の手法に関する最新の考え方を示したＣＯＳＯの「リスク評価の実務　Risk Assessment in Practice」(2012年）を輪読し、リスク評価の基本的な手法の習得に努めました。

２．本報告書の目的と特徴

①本報告書の目的は、リスク評価を内部監査に活用するための手法を提示することです。そのため、リスク評価の活用事例として、リスク評価の具体的なノウハウ、問題のある事例、および良好な事例について、**25 の「具体的事例」**を紹介すると共に、**「内部監査での活用方法／確認事項／改善提言」**を示しました。
②リスクの評価基準として、「顕在化に至る速度」と「対応策の有効性」を取り上げ、適用事例を紹介しました。
③被監査部門の内部統制、リスクマネジメント、さらには全社的リスクマネジメント（ＥＲＭ）を評価し、改善提言するという内部監査の**実務に活用**できるように努めました。

３．使用上の注意

①**本報告書は、前述の通りリスク評価を内部監査に活用するための１つの手法を提示したものであり、評価方法を網羅的に紹介するものではありません。**あくまでも、多々ある手法の事例の１つとして参照願います。

②本報告書の記載内容に関する責任は、全て本研究会にあることにご留意願います。
③本報告書に記載した事項の全てを満たす必要はなく、自社で活用できる項目から活用し、自社の現在のリスクマネジメントやＥＲＭの状況を出発点として、高度化していくことが大切です。

４．研究会メンバー　（ＣＩＡフォーラム　Ｎｏ.a3　ＥＲＭ研究会（第９期））

No.	氏名	会社名等	所属・役職
1	吉野 太郎	東京ガス(株)	リビング企画部ライフパル監査役チーム・担当副部長
2	野口 正文	損害保険ジャパン日本興亜(株)	監査役室・主査
3	藤枝 繁	みずほ情報総研(株)	業務監査部システム監査室・参事役
4	坂井 香苗	NEC マネジメントパートナー(株)	リスクアドバイザリー事業部　内部監査サービス第二部・監査マネージャー
5	紀谷 倫有	個人会員	
6	宮内 隆行	住友化学(株)	内部統制・監査部・主席部員
7	村井 直樹	個人会員	私立大学事務局職員
8	吉岡 靖之	個人会員	監査役室長
9	真柳 元	ジャパンベストレスキューシステム(株)	常勤監査役
10	丹羽 珠希	(株)三井住友銀行	監査部・上席考査役
11	有村 祥一	(株)日本政策投資銀行	監査部・参事・内部監査担当
12	小堀 真	(株)大和総研	内部監査部・次長
13	伊藤 裕美子	NECネッツエスアイ(株)	経営監査部・担当課長
14	樫原 忠	キリンホールディングス(株)	グループ経営監査担当・主査
15	宇田 文顕	SCSK(株)	リスク管理部リスク管理課・課長
16	斉藤 千春	オザックス㈱	監査室副室長
17	田中 宏	大正製薬(株)	監査部・参事
18	大島 誠	第一屋製パン(株)	常勤監査役
19	石井 学	KDDI(株)	リスクマネジメント本部・課長補佐
20	今井 俊雅	個人会員	
21	省略	省略	省略
22	和田 有弘	出光興産(株)	内部監査室・室長付
23	鈴木 均	オリンパス(株)	内部統制統括部・内部統制企画担当部長
24	成繁 新治	楽天(株)	内部監査部・課長

５．本研究会の活動の経緯

本研究会は2004年4月から活動を開始し、９期にわたり、全社的リスクマネジメント（ＥＲＭ）を内部監査に活用する手法を研究し、内部監査の質的向上に微力ながらも貢献していきたいとの思いで活動を続けてきました。その間の研究成果とその概要は以下のとおりです。

活動期間	研究成果（報告書）	概要
第１期 2004年4月 ～2005年2月	**ＥＲＭのよくある質問集（ＦＡＱ）**	ＥＲＭについて理解を促進するためのＦＡＱ。
第２期 2005年4月 ～2006年3月	**使えるＥＲＭ（全社的リスクマネジメント）導入チェックポイント集** ～ 一目でわかるＥＲＭと内部統制の基本的要素の具体例 ～	ＥＲＭの８つの構成要素が有効に機能しているかどうかのチェックポイントと、その具体的な事例。
第３期 2006年4月 ～2007年4月	**ＥＲＭ実施体制を構築するために必要な１０の要件**	ＥＲＭ実施体制構築の要件と、その具体的事例、および中小企業であっても行うべきＥＲＭの最低要件。
第４期 2007年5月 ～2008年7月	**法対応の内部統制から価値創造のＥＲＭ（全社的リスクマネジメント）へ** ～ 会社法と金融商品取引法対応の内部統制を活かしたＥＲＭづくりへの提言 ～	内部統制法制化への対応で得られた成果のＥＲＭ実施体制構築への活用。
第５期Ａ分科会 2008年10月 ～2010年1月	**ＥＲＭ的な視点を取り入れた内部監査の手法** ～ ＥＲＭの視点を活用して、企業目標の達成に寄与し付加価値を提供する内部監査を行うためのノウハウ ～	内部監査にＥＲＭ的な視点を取り入れ、内部監査の質を高め、企業目標の達成に寄与するための手法･ノウハウ。
第５期Ｂ分科会 2008年10月 ～2010年1月	**格付会社のＥＲＭ確認項目を用いた事業会社向けＥＲＭチェックリスト** ～ 事業会社の目線に立った格付会社のＥＲＭ確認項目の読替と解説～	格付会社が公表している情報を参考に我が国の一般事業会社を対象としたＥＲＭの取組状況を確認するための項目についての解説。
第６期 2010年4月 ～2012年6月	**「ＣＯＳＯ　内部統制モニタリングガイダンス」に基づいた** **ＥＲＭモニタリング事例集**	「ＣＯＳＯ内部統制モニタリングガイダンス」の手法や考え方を反映させたＥＲＭのモニタリング事例集。
第７期 2012年8月 ～2014年10月	**全社的リスクマネジメント（ＥＲＭ）を活用した内部監査手法の研究** ～「リスク選好・リスク許容度」、「主要リスク指標」、「戦略的優位性を確保するＥＲＭ」についての業種別事例とリスクベース内部監査への活用事例～	「リスク選好・リスク許容度」、「主要リスク指標」、「戦略的優位性を確保するＥＲＭ」に関するＣＯＳＯの３つのレポートから、それらの業種別の具体的事例、および内部監査における確認事項と内部監査の実務で役立つ視点をまとめたもの。
第８期 2015年2月 ～2015年11月	**改訂版ＣＯＳＯ内部統制フレームワークの内部監査での活用事例** ～改訂版COSOの17の原則の観点から見た内部監査において留意すべき問題事例と改善提言のための確認事項～	17の原則ごとに「具体的視点」を例示し、「内部監査において留意すべき問題事例」と「改善提言のための確認事項／改善提言」を説明。

第９期（当期） 2016 年 2 月 ～2016 年 11 月	**リスク評価手法の内部監査での活用事例（本報告書）** ～内部監査での活用方法・改善提言のための確認事項～	リスク評価の具体的なノウハウ、問題のある事例、および良好な事例について、「具体的事例」を紹介すると共に、「内部監査での活用方法・確認事項・改善提言」を紹介。

（注）上記報告書は全て、社団法人　日本内部監査協会のホームページの「ERM 資料集」コーナー（http://www.iiajapan.com/data/ERM_TOP.htm）上で公開されています。

Ⅱ．報告書作成の過程で得られた知見

１．リスク評価全般に関する普遍的な知見

（１）４つのリスクの評価基準

・リスクを評価するための評価基準は以下の４つがあると考えられます。
①影響度
②発生可能性
③**顕在化に至る速度**
④**対応策の有効性**

（２）評価基準の使い方

・第１段階:まず、リスクの**影響度**と**発生可能性**の組み合わせで、対応すべきリスクの候補を選択します。（このためのツールがリスクマップやヒートマップです。）
・第２段階:次に、選択されたリスクの候補から、**顕在化に至る速度**と**リスク対応策の有効性**の観点から優先的に対応すべきリスクを特定していきます。

（３）リスク評価の際の視点

・リスク評価の際の視点には、以下の３つの視点があると考えられます。
・いずれも平時から必要な備えをしておくものです。

リスク評価の際の視点	内　　容	主に関係する評価基準			
		影響度	発生可能性	顕在化に至る速度	対応策の有効性
①顕在化の予防	・リスクが顕在化しないよう、リスクが**発生する可能性を減らす**。 例：㋐手入力からシステム入力への変更（オペレーションの自動化）、㋑職務の分離など職務分掌の設定		○		○
②損失の低減・移転	・リスクが顕在化した場合の**影響度**（損失など）**を低減**する／もしくは**影響度が甚大となることを防ぐ**。 例：㋐BCP の策定、㋑建物・設備の耐震補強、㋒システムの二重化、㋓供給のバックアップ協定の締結、㋔保険の付保	○			○
③早期の把握	・リスクが顕在化する**予兆を把握**する／もしくは顕在化したリスクを早期に**把握**する。			○	○

	例：㋐各種先行指標のモニタリング、㋑リスク情報のエスカレーションルールの策定・徹底				

２．リスク評価の事例の 6 つの類型

・本報告書の 25 の事例は、以下の 6 つに類型化できる。

（１）リスクの数値化の事例　（3 件）

	表　　題	No
①	リスク評価の 4 つの評価基準を用いたリスク重要性の評価　～影響度・発生可能性・顕在化に至る速度・対応策の有効性による評価	1
②	㋐「リスク要素」の抽出→㋑「関連テーマ」の紐付け→㋒「リスク・ファクター」の評価によるリスクの重要性評価	2
③	「保有しているリスク」と「顕在化したリスク」の評価結果を用いたリスクマップによるシステムリスクの評価方法	3

（注）「No」欄に記載の番号は、本文中の通し番号（１～25）を示す（以下同じ）。

（２）リスクの顕在化に至る速度の適用事例　（4 件）

	表　　題	No
①	債権回収不能等の回収事故発生時の「顕在化に至る速度」と「対応策の有効性」を考慮した債権回収リスクの評価方法 （注）下記（３）①と同一事例	5
②	「顕在化に至る速度」の違いを踏まえた地震と感染症のリスク評価方法の違い	6
③	「顕在化に至る速度」が極めて遅いデータ改ざんリスクの評価方法	7
④	金融機関における信用リスク評価手法	15

（３）リスクの対応策の有効性の適用事例　（3 件）

	表　　題	No
①	債権回収不能等の回収事故発生時の「顕在化に至る速度」と「対応策の有効性」を考慮した債権回収リスクの評価方法 （注）上記（２）①と同一事例	5
②	標的型ウイルス感染時の情報漏洩リスク評価の誤り	19
③	「対応策の有効性」が急激に低下するリスクの評価	23

（4）固有リスクと残存リスクの活用事例　（2 件）

	表　　題	No
①	統制の段階別でのリスク評価	4
②	残存リスクのみに限定したリスク評価	9

（5）リスク評価方法・ノウハウの事例　（12 件）

	表　　題	No
①	発生可能性は低いが影響度が甚大なリスクをリスクマップで評価する場合の留意事項	8
②	内部監査部門と被監査部門のリスク評価結果の比較による重点監査項目の決定	10
③	交通事故へのリスク対応状況の評価	12
④	親会社内部監査部門から出向した子会社監査役を活用することによる企業集団のリスク評価の品質向上	13
⑤	完工までに長期間を要しその間の各段階でリスクが変化する建設業におけるリスク評価手法	14
⑥	専門家の評価の不適切な利用による埋蔵量評価の誤り	16
⑦	知見のない高度先端技術分野でのリスク評価の誤り	17
⑧	社長発案の大型投資案件に対する不十分なリスク評価	20
⑨	海外の現地企業の買収に伴うリスクへの対応	21
⑩	セキュリティ管理の対象外となっている特定用途向きパソコンのリスク評価の不備（未登録・暗号化未済・機密情報保管）	22
⑪	責任者全員への記名式リスク調査　～一般的なリスク評価手法の適用が難しい大学固有のリスクの評価事例	24
⑫	企業グループ全体でのリスク管理手法の展開	25

（6）その他　（2 件）

	表　　題	No
①	リスク評価に不慣れなメンバーが多い内部監査部門でのスキル向上策	11
②	増資引受先の持つリスク評価の未実施	18

（合計 26 件）　※うち 1 件は同一事例が 2 つの類型に該当するため事例は 25 件である。

Ⅲ．内部監査での活用事例

１．リスク評価のノウハウ　　（計 15 項目）

（１）重要度の算定手法　（4 項目）

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
1	**リスク評価の４つの評価基準を用いたリスク重要性の評価～影響度・発生可能性・顕在化に至る速度・対応策の有効性による評価**	・ある製造業の内部監査部門では、下記のリスク評価結果に基づき、監査計画を策定している。 **①評価基準** **ⓐ影響度** ㋐売上損失　（1（小）～3（大）の 3 段階評価） ㋑財産損失　（同　上） ㋒賠償責任　（同　上） ㋓人的損害　（同　上）　※㋐～㋔のうち最大値を選定 ㋔企業イメージ毀損　（同　上） **ⓑ発生可能性**　（同　上） **ⓒ顕在化に至る速度**　（1～5 の 5 段階で最低 0.9～最大 1.4 の指数評価） **ⓓ対応策の有効性**　（1～5 の 5 段階で最低 0.8～最大 1.2 の指数評価） ※具体的な評価基準は**【図表１－①】**を参照。 **②リスクの評価** ・ⓐの最大値×ⓑ×ⓒ×ⓓ ※評価のイメージは**【図表１－②】**を参照。 **［事例から得られた知見］** ・リスク評価については、従来から、「影響度」と「発生可能性」の２つの評価基準による評価がなされていたが、**新たに「顕在化に至る速度」、「対応策の有効性」を加える**ことにより、より適切な評価が可能になる。 ・特に国際的な規制の強化に対しては、例えば米国の腐敗防止法では多額	（活用方法） ・左記の通り。

		の賠償金が課されるが、リスクが顕在化する速度は早いものがあり、**「顕在化に至る速度」を評価基準に取り入れる**ことにより、より適切なリスクの評価が可能となる。	

【図表１―①】

リスク評価の４つの評価基準

ⓐ影響度

細　目	ランク	説明	定義	評価指数
㋐売上損失	3	大	全社的に大きな被害（50 億円以上）	3
	2	中	全社的な被害（1－50 億円）	2
	1	小	全社レベルに至らない（1 億円未満）	1
㋑財産損失	3	大	全社的に大きな被害（50 億円以上）	3
	2	中	全社的な被害（1－50 億円）	2
	1	小	全社レベルに至らない（1 億円未満）	1
㋒賠償責任	3	大	全社的に大きな被害（50 億円以上）	3
	2	中	全社的な被害（1－50 億円）	2
	1	小	全社レベルに至らない（1 億円未満）	1
㋓人的損失	3	大	全社的に大きな被害（50 億円以上）	3
	2	中	全社的な被害（1－50 億円）	2
	1	小	全社レベルに至らない（1 億円未満）	1
㋔企業イメージ毀損	3	大	全社的に大きな被害（50 億円以上）	3
	2	中	全社的な被害（1－50 億円）	2
	1	小	全社レベルに至らない（1 億円未満）	1

ⓑ発生可能性

ランク	説明	定　義	評価指数
3	高い	毎年、もしくは 2～3 年に 1 度	3
2	中程度	5～10 年に 1 度	2
1	低い	30～50 年に 1 度	1

ⓒ顕在化に至る速度

ランク	説明	定　義	評価指数
5	非常に速い	・非常に急激に発症。 ・ほとんど、あるいは全く警告がなく、即時。	１．４
4	速い	・数日から２，３週間のうちに発生	１．３

3	中程度	・２，３ヶ月のうちに発生	１．２
2	遅　い	・数ヶ月のうちに発生	１．１
1	非常に遅い	・非常に遅い。 ・一年またはそれ以上	０．９

※減ずるためにコンマ以下の評価指標を設定。

ⓓリスク対応策の有効性

ランク	記述	定義：現状分析として	評価指数
5	とても低い	・対応策が実行されていない、または正しく計測されていない ・リスクの説明能力の欠如、経営者の理解力の欠如	１．２
4	低い	・キーとなる対応策は実行されている。 ・リスクの説明力が低い、経営者の理解力が低い	１．１
3	中	・中程度	１．０
2	高い	・対応策は概ね実行されている。 ・緊急時のリスク対応策は正しく計画され、訓練も実施している。	０．９
1	とても高い	・戦略の全ての対応策が正しく選択されている。 ・全社でリスクの理解がされリスクへのテストや、定期的な訓練を実施している。	０．８

※減ずるためにコンマ以下の評価指標を設定。

【図表１―②】

「影響度」「発生可能性」「顕在化に至る速度」「対応策の有効性」に基づくリスク評価のイメージ

No.	部門	リスク	影響度 ⓐ						発生可能性	顕在化に至る速度	対応策の有効性	評価結果	ランク
			売上損失	財産損失	賠償責任	人的損失	企業ｲﾒｰｼﾞ損失	経営への影響					
								MAXⓐ	ⓑ	ⓒ	ⓓ	ⓔ＝MAXⓐ×ⓑ×ⓒ×ⓓ	
1	営業本部	海外子会社が米国腐敗防止法（FCPA）で提訴される	2	1	3	1	2	3	2	1.4	1.2	10.08	A
			大	小	大	小	小	大	中	非常に速い	とても低い		

【図表１－　③】

評価結果に基づくランク付け

評価結果	ランク	対応重要度
１０以上	A	大
５以上１０未満	B	中
５未満	C	小

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
2	**㋐「リスク要素」の抽出→㋑「関連テーマ」の紐付け→㋒「リスク・ファクター」の評価によるリスクの重要性評価**	・金融機関向けシステムを受託しているA社では、下記のリスク評価結果に基づき、監査計画を策定している。 **①「リスク要素」の抽出・「関連テーマ」の紐付け** ・中期経営計画、および内外環境の変化等を考慮して**「リスク要素」を抽出し、「関連テーマ」を紐付ける**と共に、その**影響度**（大・中・小）、リスク（不具合）の**発生可能性**（高・中・低）、を**評価**する。 ・なお、影響度、発生可能性が小、低のリスク要素は対象外とする。（影響度・発生可能性を評価対象とするのはこの段階まで） **＜「リスク要素」ごとの「関連テーマ」の例＞** **ⓐリスク要素：大規模システムの更改・構築の不備** **関連テーマ：システム開発・運用　※** 影響度　　：大 発生可能性：低 **ⓑリスク要素：　サイバーセキュリティ対策の不備** **関連テーマ：サイバーセキュリティ** 影響度　　：大 発生可能性：低 **ⓒリスク要素：　外部委託先の破綻** **関連テーマ：外部委託先管理** 影響度　　：中 発生可能性：低 **②「リスク・スコア」の算出（リスクの重要性評価）** ・**各関連テーマに対して、合計100%となるようにウエイト付けした「リスク・ファクター」を設定**し、（リスク・ファクター）それぞれを１から５の**5段階で評価**して、**リスク・スコア**を算出する。 **＜「リスク・ファクター」の例　　※システム開発・運用の場合＞** **リスク・ファクター　　評価** **①利益率**　（40%）　3 **②コスト削減効果**　（30%）　5	（活用方法） ・中期経営計画、および内外環境は変化するため、期初に想定した**「リスク要素」**を、**上期終了時点で確認**し、見直しや追加の要否を検討する。 ・同様に、**「リスク・ファクター」**についても、5段階の評価やウェイト付けが上期終了時点で妥当であるか確認する。 ・リスク・スコアを再計算し、上位10位のテーマに変動がある場合は、下期の監査計画を見直す。

		③保守容易性　　（20%）　　5 ④コンプライアンス（10%）　　1 合　計　　（100%） ・リスク・スコア＝３×40%＋５×30%＋５×20%＋1×10%＝３．８ ③監査対象テーマの選定 ・関連テーマ毎に算出した「リスク・スコア」を比較し、スコアの高い上位 10 テーマを監査対象とする。 ［事例から得られた知見］ ・経営目標、外部・内部環境の変化を考慮してリスク要素を洗い出すことにより、想定するリスクの影響度、発生可能性の根拠が明確になる。 ・また、根拠が明確になっているため、期中に見直しを行う際も、外部・内部環境の変化の当初想定との差異を分析することで、見直しの理由を明確にすることができる。	

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
3	**「保有しているリスク」と「顕在化したリスク」の評価結果を用いたリスクマップによるシステムリスクの評価方法**	・Ａ社は他社のシステム開発から情報システムの受託運用までを担うSI（system integration）(注1)ベンダーであり、障害やオペレーションミス等に伴うシステム停止や情報漏洩等は、会社のブランドの毀損や信頼を失墜させるため、受託**システム毎の脆弱性を認識し、適切にコントロール**することが求められる。 ・そのため、所管部は受託システムのシステム管理(注2)で要求される管理基準に従い、運用開始時点と年次のタイミングで、㋐管理基準に対するコントロールの適切性の自己評価（CSA）、㋑システムが保有する情報価値(注3)と情報量、㋒システム属性(注4)、および㋓障害・オペレーションミス・情報漏洩等の発生事案の頻度から、**保有しているリスクと顕在化したリスクの評価**を行い、監査対象とするシステムを決定する。 （注１）顧客の業務内容を分析し、問題に合わせた情報システムの企画、構築、運用などを一括して行なうこと。 （注２）運用管理体制、オペレーション管理、機器管理、アクセスコントロール等。 （注３）個人情報、機微情報、口座・カード情報　等 （注４）可用性、システム規模、・ユーザ数　等 ・保有しているリスクと顕在化したリスクの評価は、**システム毎**（①～⑨）に下記の手順で行う。 **(a)保有しているリスクの評価方法** ・（システム毎に）㋐**情報価値に関する約10項目のリスク**、および、㋑**システム属性に関する約10項目のリスク**の重要度を5段階で評価し、全項目の評価結果を合算した合計値により評価する。 **＜情報価値に関する「個人情報」の5段階評価の例＞** 100万件以上⇒５、50万件以上⇒４、10万件以上⇒３、 1万件以上　⇒２、 1千件以上⇒１ **＜システム属性に関する「可用性」の5段階評価の例＞** 停止不可⇒５、数時間以内⇒４、半日以内⇒３、	（活用方法） ・システムリスクに関する監査での監査対象システムの決定で活用する。 ①原則として**保有しているリスクと顕在化したリスクの評価結果の合計値の高い順**から監査対象とするが、合計に明らかな相違が見られない場合は、リスク対応の脆弱性を重視し顕在化したリスクが高いシステムを優先して監査対象とする。 ②年度末時点では**前年度のヒートマップとの変動**を評価・分析し、保有しているリスクと顕在化したリスクの合計値または、保有しているリスク、顕在化したリスクのいずれかの**変異が大きいシステム**について、優先的に次年度の監査対象システムとする。 ③監査テーマが**情報漏洩リスク**を目的とする場合では、保有しているリスクと顕在化したリスクの合計よりもむしろ、保有しているリスクを構成する情報価値と情報量が高いシステムを監査対象とするなど、テーマに応じた監査対象の決定にも活用する。

		翌営業日⇒２、１週間以内⇒１ ・**システム毎に、リスク**（リスク 1～リスク n）**の評価結果を合計**して、保有しているリスクの重要性を評価する。（**【図表２－①、②】参照**） **(b)顕在化したリスクの評価方法** ・**㋐CSA による約 200 項目のコントロールの充足率**、および、**㋑障害等の発生件数**に基づき、保有しているリスク同様にリスクを5段階で評価し、全項目の評価結果を加算した合計値とする。 **＜CSA による「コントロールＡの充足率」の 5 段階評価の例＞** コントロールＡの充足 50%以上⇒５、60%以上⇒４、70%以上⇒３、80%以上⇒２、90%以上⇒１ **＜「障害Ａの発生件数」の 5 段階評価の例＞** **障害Ａの発生件数　5 件以上⇒５、4 件以上⇒４、3 件以上⇒３、2 件以上⇒２、1 件以上⇒１** ・**システム毎に、リスク**（リスク 1～リスク n）**の評価結果を合計**して、顕在化したリスクの重要性を評価する。（**【図表２－①、②】参照** **(c)「保有しているリスクと顕在化したリスクの評価結果を用いたリスクマップ」の作成** ・保有しているリスクを X 軸、顕在化したリスクを Y 軸として、それぞれの**評価結果**をプロットした**リスクマップ【図表２－③】**を作成し、**システム毎のリスク値**を可視化し、対応の優先順付を行う。 **［事例から得られた知見］** ・システムリスクに関連する保有しているリスクと顕在化したリスクを評価し、**リスクマップとして”可視化”**することにより、**㋐リスクベース監査の実効性**の向上、および㋑リスク項目や評価の見直し・チューニング等の精緻化を通したリスク評価の高度化が図れる。 ・さらに“可視化の効果として、㋒社内の**リスクコミュニケーション**の活性化や**リスクカルチャー**の醸成が期待できる。	

【図表２－①　リスクの評価結果】

	固有リスク						残存リスク					
システム名	ﾘｽｸ1	ﾘｽｸ2	ﾘｽｸ3	・・・	ﾘｽｸn	合計	ﾘｽｸ1	ﾘｽｸ2	ﾘｽｸ3	・・・	ﾘｽｸn	合計
①	1	1	1	・・・	1	8	1	1	1	・・・	1	4
②	3	2	5	・・・	2	41	4	1	1	・・・	2	15
③	2	2	3	・・・	2	25	2	1	5	・・・	2	10
④	4	3	1	・・・	3	30	1	3	1	・・・	3	8
⑤	3	5	2	・・・	4	55	3	5	4	・・・	4	23
⑥	5	4	3	・・・	2	68	5	4	5	・・・	2	33
⑦	2	1	3	・・・	2	30	2	3	5	・・・	2	20
⑧	1	1	1	・・・	1	15	1	1	1	・・・	1	8
⑨	3	2	4	・・・	2	45	5	5	4	・・・	2	30

【図表２－②　重要性の評価基準】

	固有リスク	残存リスク
特大	60 以上　80 未満	30 以上　40 未満
大	40 以上　60 未満	20 以上　30 未満
中	20 以上　40 未満	10 以上　20 未満

【図表２－③
リスクマップによる対応の優先順付け】

大 ↑ 残存リスク ↓ 小	固有リスク 小 ← → 大			
	20	40	60	80
40	優先4	優先3	優先2 ⑨	優先1 ⑥
30		優先4 ⑦	優先3 ⑤	優先2
20		③	優先4 ②	優先3
10	⑧ ①	④		優先4

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
4	**統制の段階別でのリスク評価**	・A社は全社的なリスクマネジメントのPDCAサイクルの中で**全社的リスクマップデータベース**を活用している。 **(1)概　要** ・A社各部室は、「リスク評価ガイド」で定められた**評価項目と評価方法**（**【図表３―①】**参照）に従い、㋐信用リスク、㋑市場リスク、㋒資金流動性リスク、㋓オペリスク（事務リスク、評判リスク、人材リスク、有形資産リスク、情報資産リスク、法的リスク）の**４つのリスクカテゴリー**の中から当該部室用に選定されたリスクシナリオに基づいて、**Ａ～Ｄの統制の各段階でのリスクを評価**して、**「リスク評価表」**を作成している。 ・リスク統括部が、各部室のリスク評価表を取り纏めて、データベース化する。 ・リスクマネジメント・コミッティーでは、データベースから、リスクカテゴリー毎のリスク量の集計を行い、固有リスク、計画残存リスク等の各統制段階別でのリスク量を可視化したグラフを作成している。**【図表３－②】**参照） **(2)統制の段階別でのリスク評価** Ａ：**固有リスク**＝①影響金額×②発生頻度 ☞何の統制も行わない場合の原初のリスク Ｂ：**計画残存リスク**＝Ａ固有リスク×（100%－③現在の統制でのリスク削減効果） ☞現在の統制を100%実施した後に残るリスク Ｃ：**実績残存リスク**＝Ａ固有リスク×（100%－③現在の統制でのリスク削減効果×④統制実施率） ☞実際の統制実施率を加味した、現在、実際に残っているリスク Ｄ：**目標リスク**＝Ａ固有リスク×（100%－⑤追加の統制でのリスク削減効果） ☞新たな統制を加えた、リスクの低減目標 **［事例から得られた知見］**	（活用方法） ①以下の３つにリスクマップを活用する。 ㋐**リスクカテゴリー毎や事業本部毎の全社的リスク分布状況の把握** ㋑固有リスク･残存リスクの状況を踏まえた**リスクベースアプローチによる重点監査項目の選定** ㋒**監査リソースの配分** ②リスクベース監査では、実績残存リスク（C段階）が高いところが最優先されるが、それ以外にも、以下の点に注意する。 (a)固有リスクが大きいにもかかわらず、残存リスクの小さい、**リスク削減効果の大きいリスク削減策**については、その有効性を検証する。 (b)大きなリスク削減効果のあるリスク削減策は、**好事例として、全社的に横展開**されているか。 (c)影響金額の期待値のみに注目すると、**影響金額が大きく発生頻度の低いリスク**を見落とすおそれがあるため、そうしたリスクに対して対策が準備されているか。 ③リスクベース監査の根拠となっているため、リスク評価の算定プロセスについて、**算定根拠の妥当性や客観性**について監査対象とする。 例えば、算定された損失金額が、過去の実際の損実金額を下回っていることが無いか

		・**事業部門別やリスクカテゴリー別などの切り口でクロス集計**が可能（**【図表３－②】**参照））で、様々な括りでリスクの所在を確認しやすい。 ・また、年度毎の時系列データを蓄積し、カテゴリー別のリスク量の増減趨勢についても分析できる。	など。

【図表３―①】

「リスク評価ガイド」で定められた評価項目および評価方法

①影響金額

・大きなリスクは算定根拠の数値も明記する。小さなリスクは概数でよい。

＜影響金額と１の後の０の数＞

㋐影響甚大→6～5、㋑影響大→4（1 人・年）～3（1 人・月）、㋒影響軽微→2（1 人・数日）、㋓影響微小→1（1 人・数時間）～0（１人・数十分）

※影響無しは単純に０　　（例）影響軽微＝100（千円）

②発生頻度

・統制がないと発生する危険がある年間回数を推測して記載する。

・評価に至った具体的なロジックが分かるようにする。

＜発生間隔と１の後の０の数＞

㋐数十秒→6、㋑数分→5、㋒1 時間→4、㋓8 時間→3、㋔数日→2、㋕月→1、㋖年→0、㋗10 年→-1、㋘百年→-2、㋙千年→-3

（例）数日＝100（回/年）、百年＝0.01（回/年）

③現在の統制でのリスク削減効果

・現在の統制を完全実施することによって当該リスクをどの程度削減できる見込みかを記載

＜削減率のイメージと評価値％＞

㋐完全削減→100%、㋑9 割削減→90%、㋒8 割削減→80%、㋓半減→50%、㋔2 割削減→20%、㋕1 割削→10%、㋖削減不能→0%

④統制実施率

・現在の統制でのリスク削減がどの程度実現できるかを％で記載。

＜イメージと実施率％＞

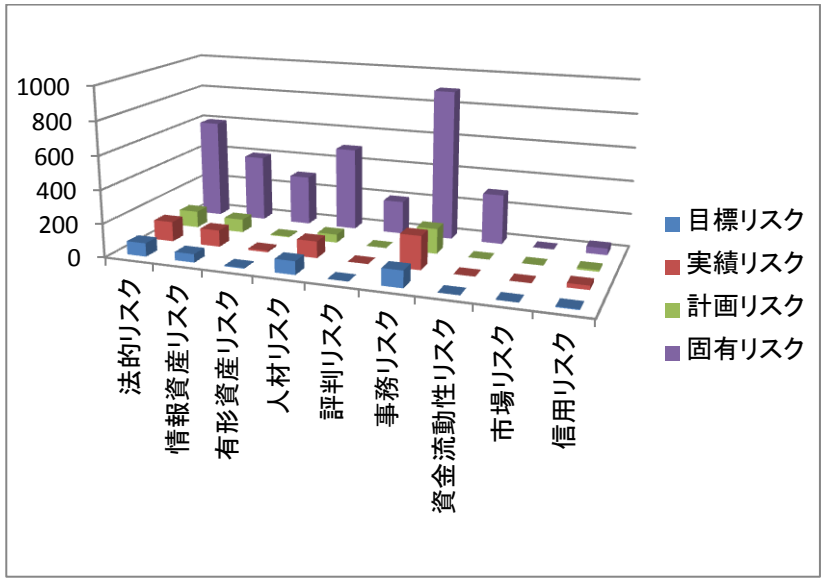
㋐完全実施→100%、㋑軽微不備→98%、㋒９割実施→90%、㋓半分実施→50%、㋔３割実施→30%、㋕実施皆無→0%

⑤追加の統制でのリスク削減効果

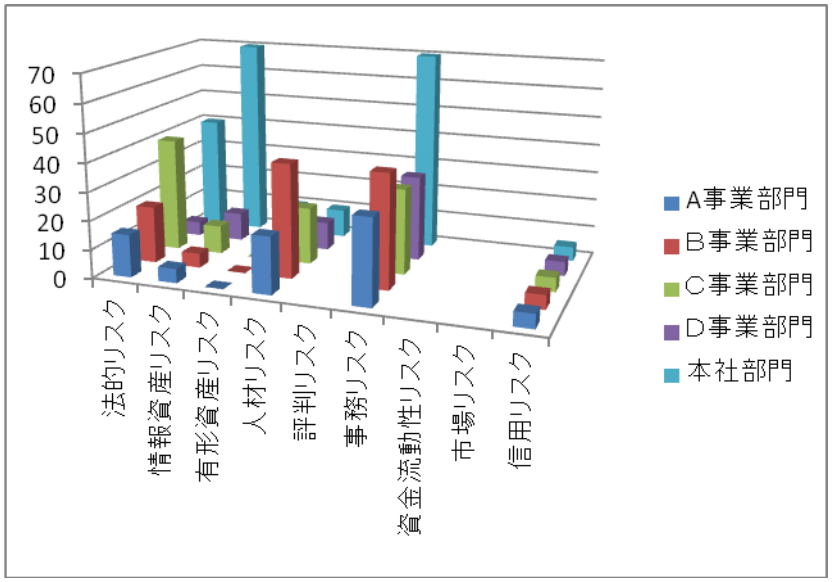
・追加で統制を増やす場合に、“追加の統制でのリスク削減効果”がどの程度見込めるかを％で記載。（0～100％）

【図表３－②】

リスクカテゴリー別の切り口でのクロス集計



事業部門別の切り口でのクロス集計



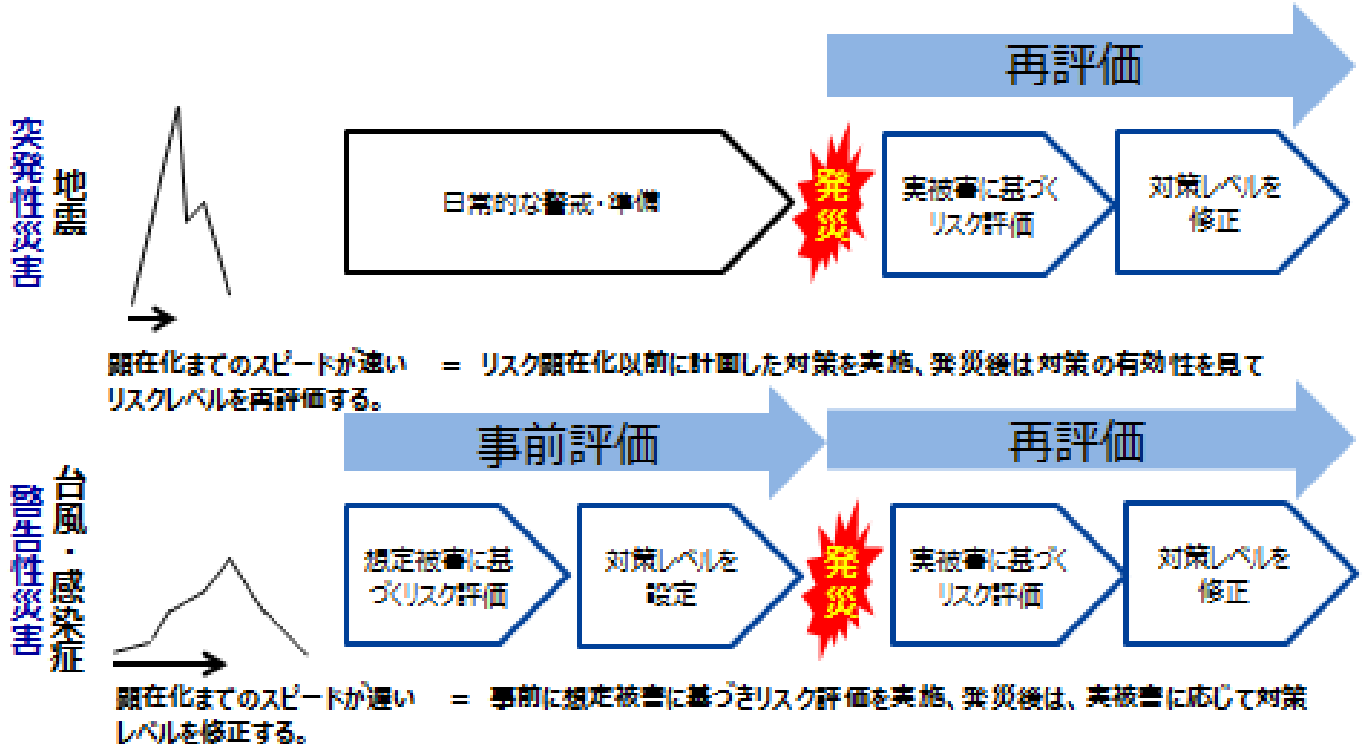
（２）評価での留意点　（5 項目）

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
5	**債権回収不能等の回収事故発生時の「顕在化に至る速度」と「対応策の有効性」を考慮した債権回収リスクの評価方法**	・**回収事故**は客先に起こるため、自社が「**発生可能性**」を低減する対策を取ることはできない。 ・**与信管理**および、**担保取得**により、事故時の「**影響度**」を一定限度内に抑えることができる。 ・しかし、回収事故は直前まで情報が隠されている（「**顕在化に至る速度**」が速い）ことが少なくないため、**客先訪問等による事故の兆候や予兆の把握**が重要になる。 ・回収事故が一旦明らかになると、他の債権者や法的処理の進捗との時間的争い（「顕在化に至る速度」が速い）になるため、**事故発生時の速やかな対応**（「**対応策の有効性**」）も重要になる。 ・「対応力」を持つ企業は、**事故発生時の有効な指揮命令や手順**が定められ、関係者は全員それを熟知しており、第一報が入った直後に各自が整斉と債権保全を実行する。 ・「対応力」を持たない会社は、事故発生時に各自が何をなすべきかが分からず、また指揮命令が混乱し、矛盾した指示が複数経路から出される。そのため、取っていたつもりの担保が破産管財人に提出され、自社の回収には使えないケースが発生する。 **［事例から得られた知見］** ・リスク対応には、事前的対応（予防的コントロール、発見的コントロール）の他に、リスクが顕在化した場合の影響を最小限にとどめる**事後的対応**があり、後者のリスク評価も重要である。	（確認事項） ・**4 つのリスク評価基準**、すなわち「影響度」、「発生可能性」、「顕在化に至る速度」、「対応策の有効性」のうち、後の２つ、すなわち**「顕在化に至る速度」、および「対応策の有効性」を踏まえた対応**を行なっているか。 **［主に「顕在化に至る速度」を踏まえた対応］** ㋐与信管理や担保管理を行なっていることに安心し、**予兆把握**が疎かになっていないか。 ㋑**事故発生時の情報伝達経路**が定められているか。 **［主に「対応策の有効性」を踏まえた対応］** ㋒**事故発生時の指揮命令系統**が定められているか ㋓**事故発生時の対応マニュアル**が定められているか。定められていても、事実上誰も知らない状態になっていないか。 ㋔担保の取得は行なっていても、**事故時の担保の活用**について検討しているか。
6	**「顕在化に至る速度」の違いを踏まえた地震と感染症のリ**	**①地震など「顕在化に至る速度」が速いリスクへの対応** ・地震など**突発性**災害では、何時、何を基準にして災害対策本部の設置などの初動対応を行うか、また何をもって終息を判断するかについて、これまで明確な**基準**がなかった。 ・従来は、震度情報（例えば震度 6）をもとに初動対応の実施を決めてい	（活用方法） ・地震や感染症など BCP 関連リスクの評価では、被害レベル（「影響度」）に加え、リスク事象の**「顕在化に至る速度」を踏まえて評価**することにより、残存リスクを正しく

	スク評価方法の違い	たが、“**遠隔地で発生した地震で自社の社員や自社工場などには影響はないが、取引先に大きな影響が出た場合**”では事前の想定と実際の対応が全く違っていた。 ・リスク評価を、従来の被害の質や大きさ（「影響度」）に加えて、**対応力**（「**対応策の有効性**）を尺度として使うことで、対策（コントロール）と残存リスクをより定量化することができた。 ・また、事前に計画していた対策の有効性が評価できるようになった。終息時期の決定もリスクレベルの変化を可視化することで対応できるようになった。 **②感染症や台風など「顕在化に至る速度」が遅いリスクへの対応** ・一方、感染症など**警戒性**災害では、事象が顕在化するまでの速度は、地震に比べて遅い。 ・したがって、事前に予防対策を打つよりも、**対策に必要な情報をタイムリーかつ正確に収集し、適切な意思決定のもと対応していく**方が有効であり効率的である。 ・さらに、リスク事象が顕在化した段階でも、**被害状況を見ながら、並行していくつかの対策シナリオを準備**できる。 ・**リスクの評価を多段階で行う**ことで、臨機応変で無駄のない対策を行うことが可能になった。 ・正確かつタイムリーな情報収集のためには、**平時から情報収集体制**を構築しておくことが重要である。 **［事例から得られた知見］** ・地震と感染症では、「**顕在化に至る速度**」がリスク評価に大きく影響を与える。 ・**「顕在化に至る速度」**を踏まえたリスク評価を行うことにより、リスク対応（対策の実施）がより効率的かつ、有効になる。	評価し、㋐初動開始や終息時期の決定、㋑有効な対策を行うための意思決定が可能になる。 ・とりわけ、**「顕在化に至る速度」**は、**地震のような突発性災害**の場合と、**感染症や台風などリスク事象の被害レベルがある程度予想できる警戒性災害**とでは、**リスク評価方法を変える**必要がある。（**【図表４】**参照） ・内部監査において、BCP 関連のリスクマネジメントプロセス、特にリスク評価ならびに対策の有効性を評価する時には、**「顕在化に至る速度」を十分考慮**して、対策が設計されているかを確認する。

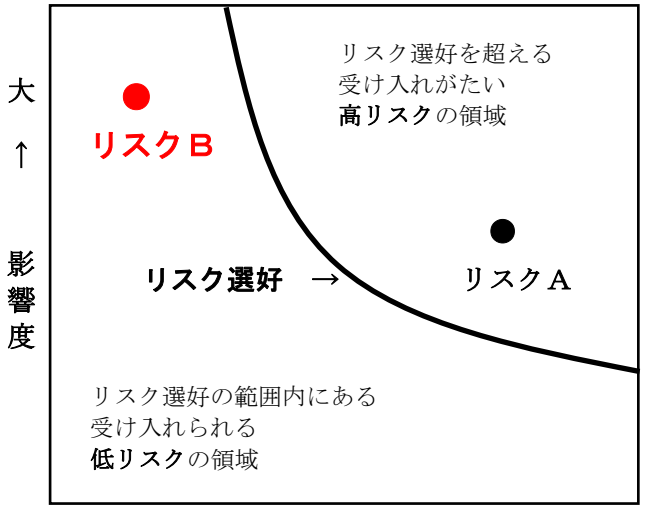
【図表４】

突発性災害と警告性災害のリスク評価方法の違い

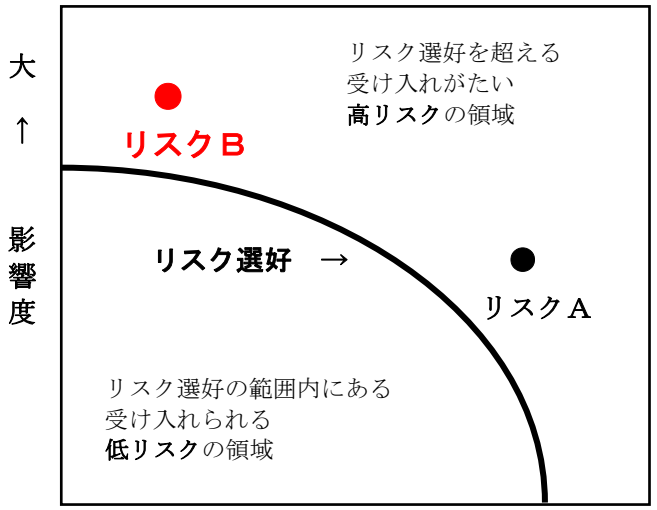


No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
7	**「顕在化に至る速度」が極めて遅いデータ改ざんリスクの評価方法**	・マンション建設時の杭打ちデータや車両燃費の算定データなどのデータ改ざん等は、長年にわたり、多数行われてきているため、顕在化した時点で初めて経営者がリスクの重大性を認識し、その時点では極めて重大な事態となっている場合が多い。 ・すなわち、**データ改ざんのリスクの「顕在化に至る速度」は、極めて遅い**という特徴がある。 **［事例から得られた知見］** ・データ改ざんリスクは、**「経営陣へのリスク情報の到達速度」は極めて遅く**、その間に損失が拡大する傾向がある。 ・そのため、リスク評価においては、**「経営陣へのリスク情報の到達速度」**という観点を取り入れる必要がある。	（活用方法） ①**リスクの種類により「顕在化に至る速度」に違いがある**ことを理解し、**「顕在化に至る速度」が遅いリスク**を、CSA、やアンケートなど幅広く情報を収集したうえで特定する。 ②特定された顕在化に至る速度の遅いリスクについて、㋐**顕在化が遅い原因・背景**、および㋑**「経営者へのリスク情報の到達速度」**を検討する。
8	**発生可能性は低いが影響度が甚大なリスクをリスクマップで評価する場合の留意事項**	・リスクマップの上で重要なリスクを選択する際に、**【図表５－①】、【図表５－②】**共に**リスクＡは重要リスク**と評価される。 ・他方、リスクＢについては、二つの考え方がある。 ㋐限られたリソースを、発生可能性が低いリスクにまで投入することは無駄となる恐れがある。 そのため、**影響度と発生可能性の双方が高いリスク**を重要リスクとする。（影響度と発生可能性を同じウエートで評価する）。（**【図表５－①】**のような選択線となる） ㋑上記㋐を基本としつつも、発生可能性は低いが**万一発生した場合には甚大な影響を及ぼすリスク**は、たとえ発生可能性が低くても、重要リスクとする。（**【図表５－②】**のような選択線となる） **［事例から得られた知見］** ・東日本大震災で巨大津波のように**発生可能性が極めて低くとも、顕在化した場合には企業の存続に影響しうるリスク**に対する検討が必要である。（対応するにしろ、対応しないにしろ）	（確認事項） ・被監査部門が行なったリスク評価を利用する場合、リスクＢについては、以下について十分なヒアリングを行なう。 ㋐リスクＢを**重要ではない**と判断した場合には、その**判断根拠**。 ㋑リスクＢを**重要である**と判断した場合には、**対応策へのリソースの投入水準**の判断根拠。

【図表５－①】



【図表５－②】



・上図は、リス　　クマップ上に事象Ａ、Ｂをプロットしたリスクのポートフォリオであり、縦軸は影響度、横軸は発生可能性を示している。

・**黒太の線がリスク選好**を示しており、**線の右上の領域はリスク選好を超える受け入れがたい高リスクの領域**を、**左下の領域はリスク選好の範囲内にある受け入れられる低リスクの領域**を表している。

・リスク選好を示す曲線は、原点から凹の線で描かれる。 ・影響度が大きくても発生可能性が低い**リスクＢは、重要性は低い**と評価。

・リスク選好を示す曲線は、原点から凸の線で描かれる。 ・発生可能性が低くても影響度が大きな**リスクＢは、重要性が高い**と評価。

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
9	**残存リスクのみに限定したリスク評価**	・A社では、監査計画策定のために行うリスク評価では、「固有リスク」と「残存リスク」の双方ではなく、**「残存リスク」のみで評価**している。 ・理由は、「固有リスク」を評価するためには、**現在のリスク対応策のリスク低減効果を除去して評価**する必要があるが、**どこまでその低減効果を除去するか**について、評価者によりバラつきが出たり、客観性・合理性を確保することが難しいためである。 ・例えば、㋐品質リスクを防止するための**品質管理マニュアルの周知・徹底**、㋑各種の**品質検査**、および㋒作業事故リスクを防止するための**各種の作業安全訓練や管理・指導**など、**既にリスク対策が日常業務の中に定着しているリスク**は、それらによるリスク低減効果を客観的・合理的に把握することは難しい。 **［事例から得られた知見］** ・**既にリスク対策が日常業務の中に定着しているリスク**については、特に固有リスクの評価が難しいため、**残存リスクで評価する**ことが適切である。 ・対応策の有効性をリスクの評価基準に取り入れる意義がここにある。	（活用方法） ・監査メンバーが**リスク評価に慣れていない**場合や、**監査経験のない特殊な業務**を監査する場合には、**「残存リスク」の評価**から開始する。

（３）内部監査部門での活用　（5 項目）

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
10	**内部監査部門と被監査部門のリスク評価結果の比較による重点監査項目の決定**	・Ａ社の内部監査部門では、監査を実施する際にリスクマップを作成しリスク評価を行っている。 ・その上で、被監査部門の部長以上に集まってもらい、投票ツールを使用したリスク評価を実施し、**双方の評価結果を比較**し、以下のようなリスクを重点監査項目としている。 **(a)監査部門は低リスクと評価したが、被監査部門では高リスクと評価したリスクでの確認事項** **①監査部門で把握していない過去の事故等がないか。** （重要問題であれば全社にエスカレーションされるが、基準以下の場合はエスカレーションされる部門が少ないため、発生可能性・影響度の把握に差が出る可能性がある。） ②監査部門として、**発生可能性や影響度の見落としはないか。** ③監査部門と被監査部門との間で、**リスクの「顕在化に至る速度」やリスクへの「対応策の有効性」についての認識に違いはないか。** ④**過去の監査時からの変更点**を確認する。 例えば、**トップの交代**や**業績の大幅な変化**があった場合、統制が有効に働いていない可能性があり、過去の監査で指摘し改善された統制でも有効ではなくなっている可能性がある。 **(b)監査部門は高リスクと評価したが、被監査部門では低リスクと評価したリスクでの確認事項** **①被監査部門が有効に機能していると認識している統制に穴はないか。運用**も**適切に行われているか。** ②**被監査部門が想定していない事象**の発生可能性や影響度を確認する。 例えば、購買部門の監査の場合の不正リスクの確認において、**バイヤー自身の不正**に対する対応策の有効性、影響度や発生可能性をどう見ているか確認する。 （一例として、バイヤーが親族の会社等を使って架空取引を行った場合を想定し、それを現状の統制でどこまで防ぐことができるか、等）。	（活用方法） ・左記の通り。

		③**過去の監査時からの変更点**を確認する。 過去に大きな問題があったが、例えば、**トップの交代**や**業績の大幅な変化**により、統制が大幅に強化された可能性がある。 **(c)双方で高リスクと評価したリスクでの確認事項** ①**有効に機能していない統制はないか。運用も適切に行われているか。** ②双方が高いと評価しているが、発生可能性や影響度の**認識に差異**はないか ③双方の間で、**リスクの「顕在化に至る速度」やリスクへの「対応策の有効性」についての認識に違いはないか。** ④上記②、③で差異や認識の違いがある場合、**被監査部門が想定していない事象**の発生可能性や影響度を確認する（逆もないか確認する）。 **［事例から得られた知見］** ・**内部監査部門**と**被監査部門**の**リスク評価結果の違い**を分析することによって、より深くリスクを評価することができる。	
11	**リスク評価に不慣れなメンバーが多い内部監査部門でのスキル向上策**	・A社の内部監査部門では、監査計画策定のために部門独自で**全社のリスク評価**を行ったが、全社的なリスク評価が初めてのメンバーが多いため、以下の順でステップを踏んで実施。 ①監査計画策定に先立って行った**経営者インタビューの結果**を、部員全員に報告し、全員の認識を共有。 ②リスク評価を初めて行う部員に対し、**リスク評価の基本的事項についての説明会**（ガイダンス）を実施。 ③部員全員を対象に、想定されるリスクや個別リスクの評価方法など**具体的なリスク評価手法についての説明会**を実施。 ④部員全員に、全社のリスクに関する**アンケート調査**を実施。（初めてのメンバーでも誤解無く回答できた。） ⑤リスク評価に関する**ワークショップ**を開催し、㋐アンケート結果を踏まえたリスク評価や、㋑メンバーのリスク評価に対する疑問点の質疑や意見交換を実施。 ⑥リスク評価を確定し、監査計画を策定。 ⑦監査計画を**経営者に説明し、結果**を部員全員に報告し、全員の認識を再度共有。	（活用方法） ・左記の通り。

		［事例から得られた知見］ ・リスク評価の理解度が不十分な監査部員が多い場合には、**ステップを踏んだ評価手法の習熟**からスタートすることによって、部員に多くの知見が得られる。	
12	**交通事故へのリスク対応状況の評価方法**	・A社の内部監査部門では、交通事故リスクを監査テーマとして取り上げ、以下の手順でリスク**対応状況の評価**を実施。 ①**関係書類の閲覧**を以下の３項目について行い、５段階評価。 ㋐事故の発生防止・損失低減策に関する社内規程の周知・徹底状況 ㋑事故発生時の対応に関する社内規程の周知・徹底状況 ㋒啓発・教育に関する社内規程の周知・徹底状況 ②**実査**を以下の３項目について行い、３段階評価。 ㋐運転者・管理者へのインタビューによる社内規程の認知・実践状況 ㋑運転日誌の査閲による社内規程の遵守状況 ㋒社有車の目視による社内規程の遵守状況 **［事例から得られた知見］** ・関係書類の閲覧では、**「仕組み」面**からリスク対応状況を評価し、実査では**「運用」面**からリスク対応状況を評価することができる ・その結果、施策立案部門と施策対象部門のそれぞれに対して、きめ細かな評価をフィードバックすることができる。	（活用方法） ・左記の通り。
13	**親会社内部監査部門から出向した子会社監査役を活用することによる企業集団のリスク評価の品質向上**	・親会社の内部監査部門では、企業集団のガバナンスの維持・向上のため、**子会社のコンプライアンスに関するリスクマネジメント**の構築・運用状況を重点的に評価している。 ・リスク評価は、同部門にて標準化された手法を子会社に適用している。 ・**標準化されたリスク評価手法の適用**により各要員のリスク評価のスキル向上とともに評価のバラツキが低減する。 ・そのため、必要に応じて**内部監査部員を子会社の監査役として出向**させ、内部監査のメソドロジーを有した**子会社監査役**が、標準化されたリスク評価手法を用いて、各社のコンプライアンスリスクを評価している。 **［事例から得られた知見］** ・子会社監査役を親会社内部監査部門から出向させることは、以下の点で	（活用方法） ・左記の通り。

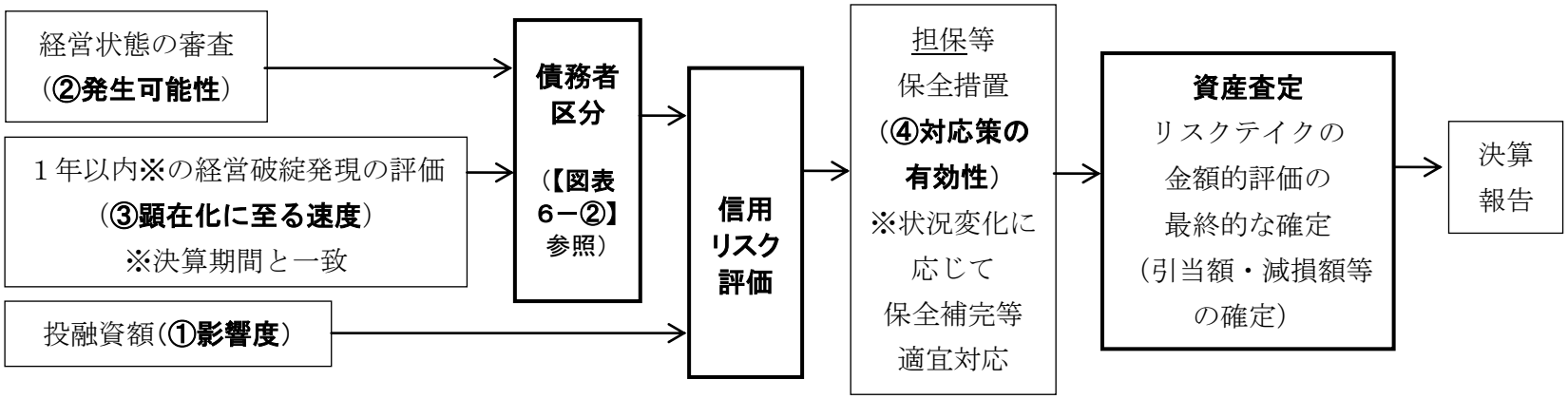
		有効。 (a)**監査のメソドロジーを有する人員を活用**できる。 (b)内部監査部門が企業集団全体の状況を把握し、必要な改善提言を行えるため、**コンプライアンスなど特定分野のリスクマネジメントの構築・運用を企業集団全体で推進**できる。 (c)**監査役監査の品質向上**。	
14	**完工までに長期間を要しその間の各段階でリスクが変化する建設業におけるリスク評価手法**	・A社はプラント建設を主とする元請会社である。 ・プラント建設では、㋐営業～契約～設計～工事の**各段階でリスクが変化する**こと、㋑**完工まで長期間にわたる**こと、㋒投資額が多額であること、㋓安全・環境に対する要求レベルが高いこと等が特徴的である。 ・**各段階での主なリスク**は以下の通り。 (a)営業段階 ☞㋐新技術の必要性、㋑顧客・協力会社の財務状況、㋒独禁法遵守 (b)契約段階 ☞㋐新技術に対する法規制、㋑追加工事・納期遅れ等に対する取決め、㋒適切な工事保険の付保 (c)設計段階 ☞㋐新技術の開発遅れ・他社技術の侵害、㋑設計ミス、㋒協力会社の経営悪化 (d)工事段階 ☞㋐建設業法遵守、㋑工事ミス、㋒工期遅れ、㋓人身事故の発生、㋔検査結果の偽装、㋕廃棄物の不法投棄 ・A社では、プロジェクトマネージャーが、チェックリストを用いて、**上記(a)～(d)の各段階ごとに、リスクを評価**すると共に、節目の進捗検討会で**問題の有無・対応策**を確認している。 **［事例から得られた知見］** ・**多段階で長期に渡る事業**では、**段階により変化するリスクの評価**が要求される。 ・蓄積した経験からリスク評価を標準化し、業務の進捗状況を日々モニタリングすると共に、新たな事象に対するリスク評価の手続きを策定しておくことが必要である。	（確認事項） ・左記の通り。

（４）その他（金融機関の場合）　（1 項目）

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
15-1	**金融機関における信用リスク評価手法** **～①影響度、②発生可能性、③顕在化に至る速度、④対応策の有効性 の視点から見た場合**	・金融機関のリスクの中核である**信用リスクの評価**プロセスについて、①影響度、②発生可能性、③顕在化に至る速度、④対応策の有効性の**４つの評価基準**に沿って整理すると次の通り（**【図表６－①】**参照）。 (a)**経営状態を審査**し、経営破綻の**発生可能性**（②）を調べ、かつ**一年以内の経営破綻発現**を評価し、**顕在化に至る速度**（③）を検討して、格付（**債務者区分、【図表６－②】**参照）を行う。 (b)一方、**投融資額**の観点から**影響度**（①）を調査し、上記(a)の債務者区分と併せて**信用リスク**を評価する。 (c)上記(b)の信用リスクに応じて、**対応策**（④）として**担保等の保全措置**を検討する。 (d)なお、上記により**リスクテイク**（残存リスク）**の金額的評価**が可能となるので、**資産査定**を行い、**引当額**や**減損額**等を確定する。	（確認事項） ・左記(a)～(d)の各プロセスが正しく実施されているか、左記と同様のステップを踏んで確認する。
15-2	**～内部監査の効率性向上への活用**	・上記(a)～(d)により絞り込まれた**リスクの大きなもの**について、重点的に監査を行う。	（活用方法） ・重点的な監査を行うことで、㋐**リスクベース**で説得力が高い内部監査結果を得られるだけでなく、㋑限られた内部監査**資源の有効活用**が可能となる。
15-3	**～顕在化に至る速度の観点の重要性**	・営業部店が**単に「経営破綻の発生可能性が高い」という理由だけで、**投融資を躊躇している（改善を要する）。 ・内部監査部門が個別債権評価において、**単に「経営破綻の発生可能性が高い」という理由だけで、**リスクを高く評価している（改善を要する）。 **[15-2、15-3 の事例から得られた知見]** ・上記①～④の程度に応じた重点的な内部監査を行うことで、リスクベースで**説得力が高い監査結果**を得られるだけでなく、限られた**監査資源の有効活用**が可能となる。 ・内部監査部門、被監査部門共に、**顕在化に至る速度**を十分検討することにより、**リスク対応策の改善による状況改善の可能性を正しく評価**することが可能となり、**短絡的な結論に陥ることを回避**できる。	（改善提言） ・たとえ現時点において、経営破綻の発生可能性が高くても、**一定の期間があれば経営改善の可能性が認められる場合**には、**リスク対応の改善**について**投融資先を支援**することにより、**融資を回収**できる可能性があることについて、営業部店・内部監査部門共に十分考慮することが必要。

【図表６－①】　金融機関における信用リスク評価・資産査定の考え方

・金融機関のリスクの中核である**債務者区分、信用リスクの評価**、および**資産査定**を、リスク評価の４つの評価基準である①影響度、②発生可能性、③顕在化に至る速度、④対応策の有効性により、概念整理すると次の通り。



【図表６－②】　債務者区分のベースとなる考え方

金融再生法 開示債権区分	考え方（実際は、各金融機関により更に細分化等定義して管理）
正常債権	業況・財務内容共に特に問題は認められない、あるいはあっても軽微な問題と考えられる。
要管理債権	当該債権が特に管理すべき状態にあると考えられる。
危険債権	今後、経営破綻状態に至る可能性が大きいと考えられる。
破産更生債権および これらに準ずる債権	法的な経営破綻等の事実が認められる、あるいは実質的に経営破たんしていると考えられる。

２．問題のある事例　　（8 項目）

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
16	**専門家の評価の不適切な利用による埋蔵量評価の誤り**	・海外の海底大深度にある資源の探鉱・開発に当たる国内企業では、試掘を行い、**業務委託先の解析専門業者の調査結果**に基づき、埋蔵量や経済合理性を評価して巨額の投資判断を行っていた。 ・本格的に掘削を進めたところ、資源は想定以下の量しか産出せず、しかも価格の下落によりプロジェクトの採算が赤字になった。今後、市況が回復しなければ、赤字が積みあがる状況である。 ・解析専門業者からの調査結果を、担当部門が解釈する際、**経験値以上の深度の試掘**に関して、**確率統計的に既存データと同一で扱っていた**ことが後日判明した。 ・価格の回復見込みを勘案した結果、投資損失処理（減損）を行い、本案件からは撤退することになった。 **［事例から得られた知見］** ・**自社の専門外の分野に関する情報**をインプットされた時、専門家の評価結果という一見合理的な根拠で社内コンセンサスを取るのではなく、判断の拠り所である「リスク評価」という原点に立ち返り、専門家から説明を受けた上で**自らリスクの「発生可能性」を吟味**するという意識行動をとらないと思考停止に陥ってしまう。（専門家の意見への盲信）	（確認事項） ①**専門家の技術情報に対する検討（吟味）**が十分であるか。（甘くないか、**盲信**はないか）。 疑問がある場合には、専門家に説明を求める。 ②投資採算性の検討において、**確率統計的な手法**に過度に依存していないか。 ③価格相場など**外部環境の見通し**は適切か。 ④シナリオ分析が客観的か。 一見、客観情報のように見えても、そこにプロジェクト推進責任者の**恣意や主観**の入り込む余地はないか。 ⑤問題に気付いてからの**経営陣への報告**は迅速か。
17	**知見のない高度先端技術分野でのリスク評価の誤り**	・甲社の乙事業部門は、**新しい高度先端技術**を活用した商品・サービスを取引先に提供する部門である。 ・内部監査部門は、当該技術に拠って立つ事業のリスクを評価するにあたって、関連した**専門的知識を持つ人材がいない**ため、専門図書は参考にしつつも、乙**事業部門の説明を鵜呑み**にしてリスクを評価していた。 ・監査担当役員・部門長も、それで已む無しと是認していた。 ・しかし実際には、技術面でも一気に陳腐化が進んで来ており、またビジネス面でも市場は拡大せず、急速に厳しい状況に追い込まれていたが、内部監査部門では、それらを把握できないまま「特段の問題を認めず」との報告を経営層に行っていた。	（確認事項） ①新技術の専門的知識を持つ人材がいない場合には、被監査部門からの説明を鵜呑みにせず、**社内外の専門的知識を持つ人材の支援・補完**等を行い、リスク評価を適切に行っているか。 ＊1 年以内に前在籍部門を監査することによる利益相反を防ぐためには、**外部の専門的知識をもつ人材を一時的に活用**する等の対応が必要となる。 また、監査担当役員・部門長も、明確にそ

		［事例から得られた知見］ ・先端技術分野のリスク評価は、状況に応じてこまめに見直しを行う必要がある。とりわけリスクの「**顕在化に至る速度**」**は一層こまめに逐次見直し**を行う必要がある。 ・専門性のある人材、とりわけリスクの「**顕在化に至る速度**」**を評価しうる人材**を確保することが必要。	れを指示しているか。 ②高度先端技術分野は、投資額が莫大な一方で、技術価値が認知されるまでは非常に狭隘な市場での戦いを耐えなければならないため、**初期段階の確認を緻密に**行っているか。 ③リスク評価を（静態的でなく）**動態的に逐次見直し**ているか。とりわけ「顕在化に至る速度」に特に注意しているか。 ④**市場撤退を含めたアクションプラン**が十分に策定されているか。
18	**増資引受先の持つリスク評価の未実施**	・食品メーカーＡ社は事業多角化の推進を進めていたが、冷凍食品市場で有数のブランドを有するＢ社より**事業提携**の話が持ち込まれた。 ・冷凍食品事業を担当する加工食品事業部は、当該事業提携は冷凍食品事業拡大を推進する好機と認識し、事業提携と引き換えにＢ社の**第三者割当増資**（10 億円程度）**を引き受け**た。 ・程なく、Ｂ社は会社更生法の適用を申請し倒産、Ａ社は増資引受額の損失を蒙った。 ・Ａ社では、株式の引き受けに関しては、社内規程上、形式的な点検は求めているものの、**デューデリジェンスの実施は任意**であったことから、今回の増資引き受けにおいても実施しておらず、Ｂ社の財務状態を的確に把握していなかった。 **［事例から得られた知見］** ・社内規程には、**“抜け穴”ともいえるような規定**がある場合がある。規程の遵守について、形式主義に陥ると、その背景にある根本思想が看過される可能性が高まる。 ・この事例は、規定の背景にあるリスクへの対応という思想が看過されたことが原因である。 ・**“抜け穴”ともいえるような規定**が看過されたままに放置される場合、規程類の形骸化が進み、リスクへの対応力（リスクの評価、対策の策定等）が低下する恐れがある。	（確認事項） ・**投資案件に関する意思決定のプロセス**を検証し、適切なものになっているか。 ・例えば、㋐関連する規程間に齟齬がないか。特に例外規定については、その内容が妥当か。㋑**金額レベルに応じてデューデリジェンスの実施**を義務付けているか、㋒投資案件の内容に応じて、**問題が発生した場合の対策**が求められるようになっているか。
19		（Ａ事業体における大規模情報漏洩事案） ・Ａ事業体が標的型ウイルスに感染した際に、以下の通り**情報漏洩に係る**	（確認事項） ・大規模情報漏洩に係るリスク評価について、

	標的型ウイルス感染時の情報漏洩リスク評価の誤り	**リスクを過小評価**。 ・大規模情報漏洩事案において、情報漏洩に係るリスク評価が誤っていた以下の事態が認められる。 ①最初にウイルスメールを職員数名が開き、パソコン数台に感染していることを検知した日に、職員宛てにメールや掲示等で注意喚起を行ったが、**ウイルス感染の影響を過小評価**した。その結果、 (a)注意喚起の内容には**具体性な「タイトル名、メール内容、添付ファイル名」**は記載されていなかった。 (b)感染したパソコンを隔離したのみで、そのパソコンつながっていた**当該部署のサーバを他のサーバから隔離**する等のシステム的対応はしなかった。 なお、この時点では、ウイルスがどのような内容のものか、判別できておらず、**外部委託先のセキュリティ会社に調査**を依頼している状況であった。 (c)数日後、セキュリティ会社より、情報流出させるタイプではないとの回答があり、**そのまま静観**した。 なお、セキュリティ会社の回答がでるまで、**当該パソコンの隔離以外のシステム的対応**は行われなかった。 ②上記①から約 10 日後、多数の標的型ウイルスメールが届き、数十台のパソコンに感染したことが判明した。 この時点で、情報漏洩リスクの再評価は行われたと考えられるが、その評価が十分ではなく、その翌日に警察へ捜査依頼は行ったものの、**インターネットとの接続を遮断**する等のシステム的対応は取られなかった。 ③上記②から更に数日後、複数の部署で**不審な通信**が確認された。しかし、そこでも、情報漏洩リスクの再評価に基づく対応を変えるに至らず、**インターネットとの接続を遮断**する等のシステム的対応の判断はなされなかった。 ④上記③から数日後、警察より情報漏洩している事実の連絡が入った。情報漏洩の事実が確定したにも関わらず、**インターネットとの遮断は即日**	以下のような監査での改善提言が考えられる。 ①-1 標的型攻撃メール等を検知した際の、**初動のリスク評価**は適切か。 **事態が判明するまで保守的（慎重）な対応**となっているか。（必要最小限ではなく、**適切な範囲を想定した対応**を行っているか） ①-2 ウイルス感染された際に、自社でその**判断の適切性を判断できる人材**を確保しているか。（**セキュリティ会社に判断を丸投げ**していないか。） ②標的型攻撃メール等が**継続的に、かつ増加**しているときのリスク評価は適切か。（ウイルス感染の可能性を高める等、**リスク評価を上げる**ことになっているか。） ③不審な通信が行われる等、自社からの漏えいが**強く疑われる場合のリスク評価**は適切か。（漏洩が確定するまででも、強く疑われる事態があれば**リスク評価を高くし**、インターネットの遮断を検討する態勢ができているか） ④情報漏洩の事実が確認された際には、**即時にインターネットを遮断する態勢**ができてい

		ではなく、その翌日であった。 ⑤インターネットとの遮断は、上記④の通りとして対外的に公表もされたが、遮断したネットワーク以外にも**インターネットに接続している古いメール専用ネット回線**があることが**見過ごされ**ており、実際は④で遮断した日より数日後まで完全な遮断は行われていなかったことが判明した。 ⑥加えて、上記⑤の事実が**監督官庁に報告**されていなかったことが、後日判明した。 （出典：ウィキペディア及び YOMIURI ONLINE の記載事例を参考に、架空の事例を作成） **［事例から得られた知見］** ・リスクが顕在化していなくても、大規模情報漏洩リスクなど**「懸念」の段階でスピード感のあるリスク対応策を取らなければならないリスク**がある。 ・**「懸念」の段階で、業務運営に支障が出かねない対応を取る**ためには、平時から**経営に甚大な影響を及ぼす可能性があるリスク**を**想定・評価**し、**顕在化した際に取るべき対応策**を**検討**し、それらについて経営者および従業員の理解を得ておく必要がある。	るか。 ⑤遮断すべきネットワークを**網羅的に把握**し、その**遮断方法が明確**になっているか） ⑥**遮断すべきネットワークを網羅的に把握**し、その**遮断方法が明確**になっているか。 ⑦情報漏洩等、重大な事態が発生した場合の**報告ライン**は問題ないか。（当局宛て報告も含め、**適時適切な報告を行う態勢**ができているか）
20	**社長発案の大型投資案件に対する不十分なリスク評価**	・企業買収や基幹システム導入など大規模な投資案件を社長によるトップダウンで推進する場合、担当部門は、社長のお墨付きがあったとして「投資ありき」で事業を進めようとしていた。 ・リスク管理部門は、投資に懸念があったが、問題点を指摘すると、社長の意向に反するのではないかと慮り、必要な意見具申を行わなかった。 ・その結果、リスク評価が不十分なまま、投資が実行され、後にリスクが顕在化する状況にあった。 **［事例から得られた知見］** ・**社長発案の大型投資案件**では、事業担当部門でも管理部門でも**リスク評価が甘くなる**ことを認識する必要がある。	（活用方法） ・**社長によるトップダウン案件**は、担当部門およびリスク管理部門共に、**リスク評価が甘くなる**ことを認識しておく。 （改善提言） ・社長主導の大型投資案件は、社長が担当部門およびリスク管理部門に対して**通常案件より厳しくリスクを評価するよう指示**する等、社長への定例／随時の監査結果報告の場で意見具申する。
21	**海外の現地企業の買**	・Ａ社は海外の現地企業の買収を計画したが、PMI（Post Merger Integration：M&A 後の経営統合）のための事前のリスク評価のうち、**現地企業の現経営陣の意向把握が不十分**で、Ｍ＆Ａ後、主要ポストを確	（改善提言） ・買収によるメリットだけでなく、**潜在的なリスクへの検討**を十分に行う。

	収に伴うリスクへの対応	保できないリスクを識別できず、その対応策を作成しなかった。 ・そのため、買収後の現地企業の**COO、CFO など主要ポスト**を確保する方向で現地企業と交渉したが、A社は海外企業の買収ノウハウに乏しく、買収後の経営体制についての合意を十分しないまま買収を実施した。 ・買収直後、現地企業の経営陣から強い抵抗を受けて**主要ポストを確保できず**、その結果、A社の現地企業への関与度合いは、当初の想定よりも低いものとなった。 **［事例から得られた知見］** ・M&A におけるリスク評価では、PMI を含めたリスク評価を行い、**最悪のシナリオに基づく対応策**までを網羅的に作成することが必要である。	・検討にあたっては買収の直接の実施部署だけでなく、コーポレート部門を巻き込んでチーム編成する等、**社内横断的な体制**を構築する。 ・想定外の状況変化が発生した場合は、経営層に迅速に、状況を報告する。
22	**セキュリティ管理の対象外となっている特定用途向きパソコンのリスク評価の不備（未登録・暗号化未済・機密情報保管）**	・システム運用会社A社では、複数の顧客の EC（electronic commerce：電子商取引）(注) サイトの開発および運用業務を請け負っている。 （注）自社や他社の商品・サービスを、インターネット上に置いたウェブサイトで販売するサイトのこと。 ・A社の営業担当者Bが業務で使用しているノートＰＣが自宅で盗難されたと緊急連絡センターから報告を受けた。 ①A社では持出用のノートＰＣは**事前登録制**となっており、かつ常時持出／一時持出を区分し、任命された部門責任者が管理するルールとなっていたが、当該のノートＰＣは社内使用を前提としており、**登録管理を行っていなかった。**（運用不備） ②A社では持出用のノートＰＣには**暗号化ソフト**を導入するルールとなっていたが、当該のノートＰＣは社内使用を前提としており、暗号化処理を行っていなかった。（運用不備） ③A社では機密情報はフォルダごとにアクセス管理をされたファイルサーバーに保管し、ＰＣの**ローカル・ハードディスクには、機密情報を保管しない**様にルールが整備された。 しかし、当該のＰＣには**ルール整備前の**提案資料・要件定義、メールのバックアップなどの機密情報が保管されたままであった。（運用不備） ④営業担当者Bは、徒歩圏内にあるビルでの社内打合せのために夕方ノートＰＣをカバンに入れて持ち出した。 打合せ後に、上司に飲み会に誘われたため、自席へ戻らずそのままノート**ＰＣを自宅に持ち帰った。**	（確認事項） ・以下により「リスク対応策の有効性」を評価する。 ①-1 ノートＰＣの全数管理ができているか。 ①-2㋐全ての情報端末の登録管理、㋑未登録端末の重点管理。㋒集中購買形式での端末配布。（改善提言） ②**暗号化未処理ＰＣ**がある可能性があることを想定して、確認する。 ③-1 ルール整備の通知時に、それまで記録された**データ削除の記載**があったか。 ③-2 ルールの徹底状況を調査する。 ④-1 上司に当該ＰＣが持出し**登録されていないことの認識**があったか。 ④-2 **持ち出し登録が一目で分かるシール**の添付。および**登録状況一覧表**の定期的な配布と

		⑤営業担当者Ｂは、ローカル・ハードディスクに**どのような営業情報が入っているかを把握していなかった**ため、影響範囲の特定に時間を要し、対外公表が遅延した。 **［事例から得られた知見］** ・**情報セキュリティ管理の対象外**となっている**特定用途向きのパソコン**に対する管理状況を確認する必要がある。	上長確認。（改善提言） ① **機密情報の保管状況の確認**徹底。（改善提言）
23	**「対応策の有効性」が急激に低下するリスクの評価**	・業務監査において、具体的リスクに対して必要な規則・組織が整備され、一定期間の運用状況の検証を行い問題なければ、「適切」という判断を行うことが多い。 ・しかし例えば、㋐震災等の特需で**業務が想定外に増え**たり、㋑インフルエンザ感染者・退職者の続出などで**マンパワーが想定外に不足**したり、また、㋒それらが同時発生した場合に、**「対応策の有効性」が一時急激に低下**する可能性がある。 **［事例から得られた知見］** ・**想定外の業務増加や人員不足**等、**リスク対応策の有効性に重大な影響を及ぼす要因**のリスク評価を確実に行うことが必要。	（活用方法） ・**業務および人員の量や質の急激な低下**など、**「対応策の有効性」に重大な影響を及ぼす要因**を把握しているか。

３．良好な事例　　（2 項目）

No	表　題	具体的事例	内部監査での活用方法・確認事項・改善提言
24	**責任者全員への記名式リスク調査** **～一般的なリスク評価手法の適用が難しい大学固有のリスクの評価事例**	**（私立大学における組織の特徴とリスク評価の難しさ）** ・私立大学は、各大学固有の「建学の精神」に基づいて、教学組織（教員）とこれを支援する事務局組織（事務職員）から構成されている。 ・教学組織は、一般的に**学部単位等で独立色が強く、リスク管理もサイロ型**である。 ・さらに、各大学の**組織の運営・管理も多種多様**であるため、リスク評価の際に、同業他社比較等のベンチマーキングが難しい。 **（責任者実名アンケートによるリスク評価サーベイ）** ・教学組織および事務局組織の**責任者全員への実名によるアンケート調査**(注)を実施。 （注）例えば、「大学及び大学を取り巻くリスク調査」といった名目で。 ＜メリット＞ (a)**回答率**は 100%。 (b)記名なので**情報格差の特定**が可能。 (c)責任者による回答であり**質が高い**。 ＜留意点＞ (a)コンサル会社等の助言に基づいたアンケート調査の場合、実態に合わない**ワンパターンのリスク分野**で分類されがち。 (b)**各大学固有の組織、運営・管理の状況に適合したリスクの整理**が不十分 ・アンケート結果は集約のうえ、リスク評価が調整され、関係者にフィードバック。 **［事例から得られた知見］** ・リスク管理体制は所属する組織ごとにユニークであり、**リスク評価に必要な情報が限定**されているケースにしばしば直面する。 その場合、**様々なルートでリスク評価に利用可能な情報を収集**することが必要。	（活用方法） ①リスク評価サーベイの結果から、大学特有のリスク分野(注)と所管・関連事務局組織をマトリックスとして整理し、**全体のリスク構成**を把握する。 （注） ㋐カリキュラム（授業、教育課程編成） ㋑ディプロマ（卒業、学位授与） ㋒アドミッション（入試、入学者受入れ） ㋓研究費使用管理 ㋔学生生活支援　等 ②同時に、責任者**回答が多い分野**は、大学としてリスクが高い分野であることが推認される。 ③上記①、②で把握した全体のリスク構成とリスクが高い分野に対して、過去に監事監査および内部監査（業務監査）として実施してきた監査項目、監査対象組織をトレースする。 ④その結果、**ハイリスクであるにもかかわらず、従来監査対象から漏れていたリスク**が把握できる。

		・**リスク管理がサイロ型**であり**リスク管理統括機能が不十分**な組織でも、**組織横断的な調査やアンケート**等が実施されている場合には、それらは有効なリスク評価サーベイとして利用できる。	
25	**企業グループ全体でのリスク管理手法の展開**	・自動車メーカーA社は、グループリスク管理の一環として、**グループリスク管理委員会**を毎月開催し、取り上げられたテーマについてリスク評価を行い、その評価結果に基づく対応策を議論している。 1．出席者 ・親会社コンプライアンス部門　※事務局：部長、課長、担当者 ・グループ各社のコンプライアンス担当者　※主に部課長クラス ・外部アドバイザー　※専門的知見の提供 2．目的 （1）自動車産業のプレーヤーとしての社会的責任を果たすこと （2）レピュテーションの毀損を予防すること （3）その他事業上のコンプライアンスリスクへの対応 3．主なテーマ 製造・交通・環境関連のリスクを中心に幅広く時宜にかなったコンプライアンステーマ 4．運営 （1）社内外の事例の発生シナリオや損失額からリスク評価を実施し、そのリスク評価に基づき議論を行うことで、グループ内でリスクに対する価値観を共有する。 （2）同委員会を受けて**グループ各社**は自社でリスク委員会を開催し、**自社の状況に置きなおしたリスク評価**の実施および統制活動の設計を行っている。 **［事例から得られた知見］** ・グループ各社のリスク管理担当者が一堂に会して意見交換をすることは、グループガバナンスやグループ全体でのリスク管理の強化に貢献する。 ・グループ各社の担当者にとって、自社内に十分な相談相手がいるという状況は稀であり、**横のつながりが持てる**ことは有益である。 ・また、リスクの識別・評価を自社内だけで実施していると、どうしても漏れや偏りが生じるが、グループ横断的な会議体があることで、**相互補**	（確認事項） ・グループリスク管理委員会で共有された**グループリスク管理方針**が、どのように社内で報告・共有されているか。 （活用方法） ・**グループリスク管理委員会の議事録**を毎回確認し、グループおよび自社にとっての重点リスクや方針などを把握し、内部監査部門でのリスク評価に活用する。 ・個別監査の計画・予備調査の段階で、**グループリスク管理委員会で議論された内容**がどのように業務に取り込まれているのかを確かめ、必要に応じて監査項目として取り上げる。

		完やグループポリシーの浸透が期待でき、グループ全体のリスク管理体制が強化される。	

参考文献

①トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）著
『Risk Assessment in Practice（リスク評価の実務)』(2012年10月)
②トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）著　八田進二・箱田順哉監訳　日本内部統制研究学会 新ＣＯＳＯ研究会訳
『ＣＯＳＯ内部統制の統合的フレームワーク』(2014年2月　日本公認会計士協会出版局刊)」

以　上