

個別リスクマネジメントに横串を通す
統合リスクマネジメントからERMへ

~ Certus™ Riskの活用法 ~

GRCジャパン株式会社

GRCジャパンは、統合リスクマネジメントのためのソフトウェア『**Certus™ Risk**』（旧製品名：**Acertus Governance**）を中心として、企業や組織のリスクマネジメント体制構築とガバナンス向上に関する様々なサービスをご提供しています：

- リスクマネジメント体制構築に関わる支援、コンサルティング
- リスクマネジメント体制構築の基盤となるソフトウェアのライセンス販売およびサポート

- 設立：2006年2月
- 代表者：真島 俊明
- 資本金：4,980万円
- 所在地：東京都千代田区霞ヶ関3-7-4 明産富士ビル2階
- Webサイト：<http://www.grc-j.com/>

GRCジャパンは、主力ソフトウェアの開発元である加Securac社が、米Neohapsis社と業務統合したことにより、2008年7月に、前身であるセキュラックジャパン株式会社から社名を変更いたしました。

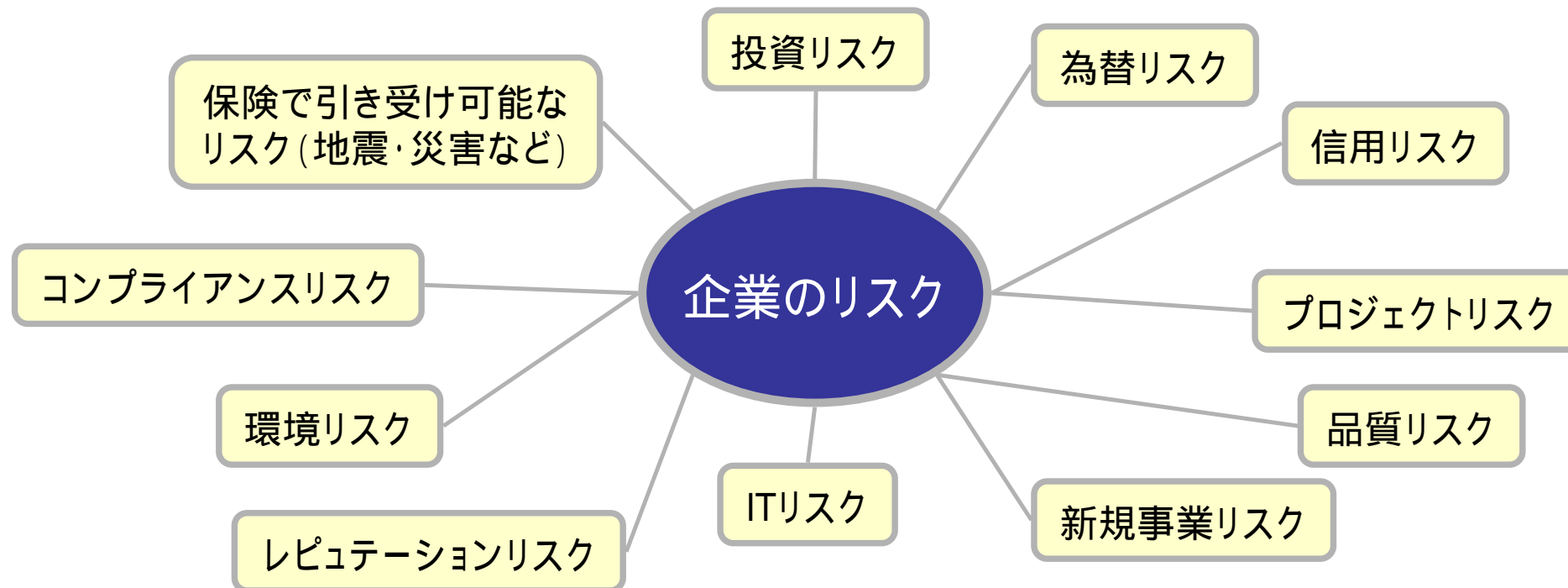
企業にとって、リスクとは...

- 組織の収益や損失に影響を与える不確実性

企業にとってリスクマネジメントとは...

- 収益の源泉としてリスクを捉え、リスクのマイナスの影響を抑えつつ、リターンの最大化を迫及する活動

出典：経済産業省『先進企業から学ぶ事業リスクマネジメント実践テキスト - 企業価値の向上を目指して - 』（2005）

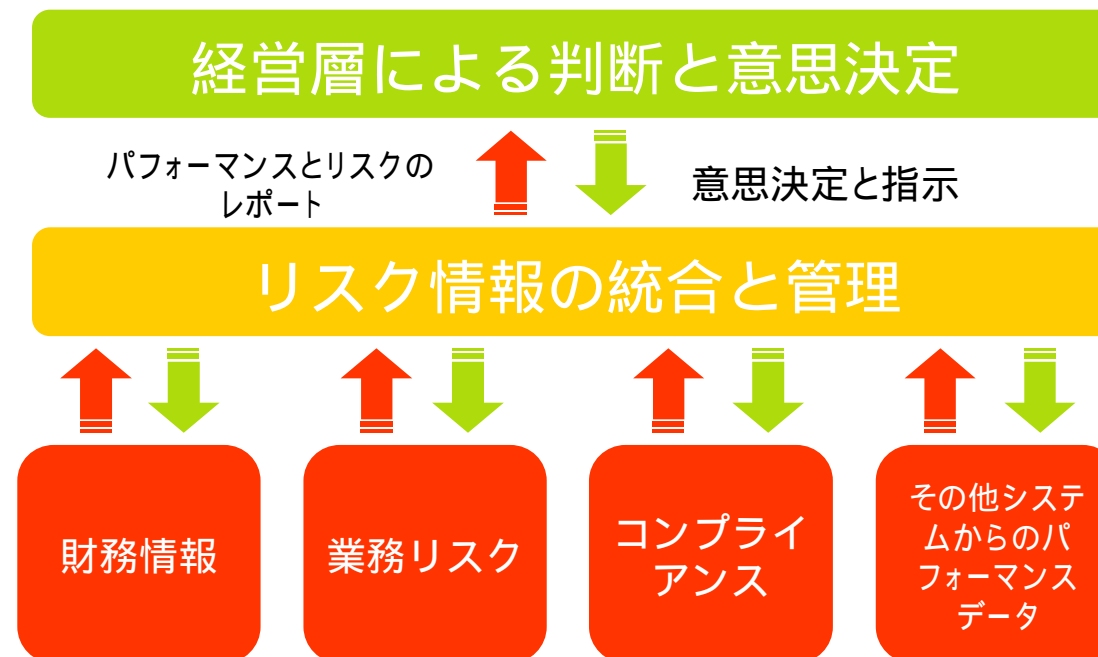


リスクマネジメントは、近年の経営環境の変化と、社会的責任の増大により、企業の経営にとって検討しなければならない最優先の課題となっている。

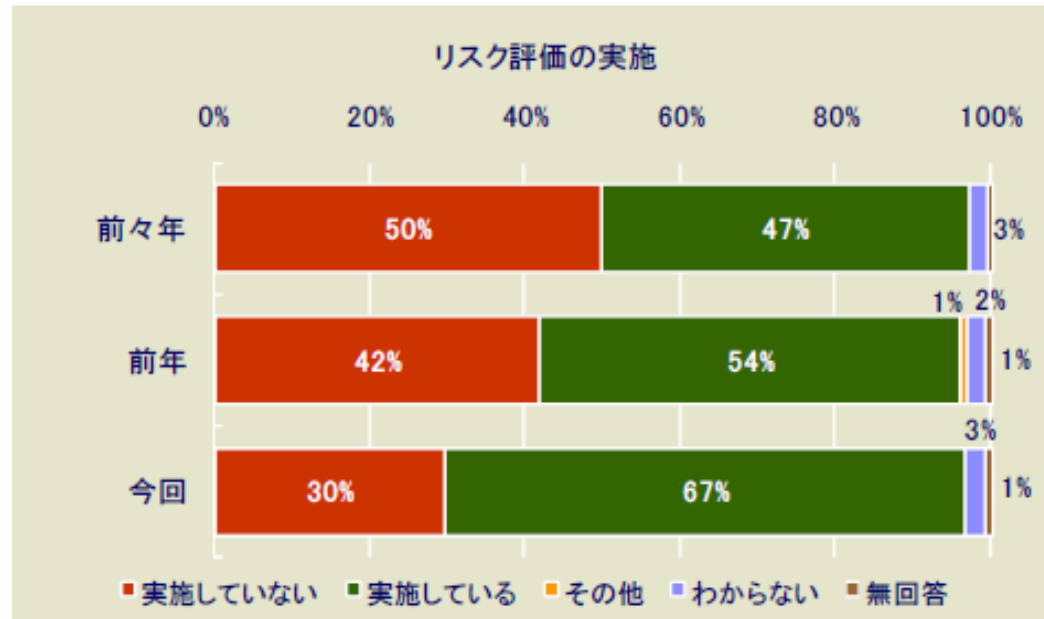
| | |
|-------------|--|
| 規制緩和の進展 | 企業の自己責任範囲の増大とともに、企業がそれぞれの判断でリスクを管理し、収益を上げていくことが必要となってきた。 |
| リスクの多様化 | 急速な技術進歩、事業の国際化、事業展開のスピードアップ、環境問題等。 |
| 経営管理のあり方の変化 | 当事者間の暗黙の了解や信頼関係のみに依存した経営管理のあり方に限界が生じてきている。 |
| 説明責任の増大 | 市場経済が進展していく中で、リスクの特定、評価や対応を怠った場合、広範なステークホルダーに損害を与えると同時に、市場の信頼を失い、企業自らも厳しいペナルティを受けることになる。 |

| | 概要 | リスクマネジメントの要求 |
|-----------------|---|--|
| 会社法 | 従来のお社に關する法律を一本化したもので、企業經營の自由化を促進する代わりに健全性確保（經營者の義務）の仕組みを規定。 | 企業の損失の危険を管理する規定その他の体制 = リスクマネジメントの構築に係わる事項が取締役会の専決事項とされている。 |
| 金融商品取引法 (J-SOX) | 証券取引法を改正したもので消費者保護のために金融商品について横断的かつ包括的に法整備。 財務報告に關する内部統制報告書の作成義務。 粉飾決算の防止、株主、投資家に対して財務諸表の正確性を確保・保証。 | 財務諸表に影響のあるさまざまなプロセスを洗い出し、誤り、改ざん、データ喪失などのリスクの発生する可能性と財務諸表の影響度を評価し、対応策を適用する。 |

- リスクを**全社的視点**で合理的かつ最適な方法で管理して**リターンを最大化**することで、**企業価値を高める活動**
- 全社のリスクマネジメント体制を構築し、**リスクに優先順位をつけて予防策を実施**すること
- 伝統的に個別に行われているリスクへの取り組みも含め、断片的な対応ではなく、**リスクに対する様々な視点を統合**し、**変化する環境に適切に対応**できるようにすること



2. リスク評価の実施



リスク評価

リスク評価に関しては

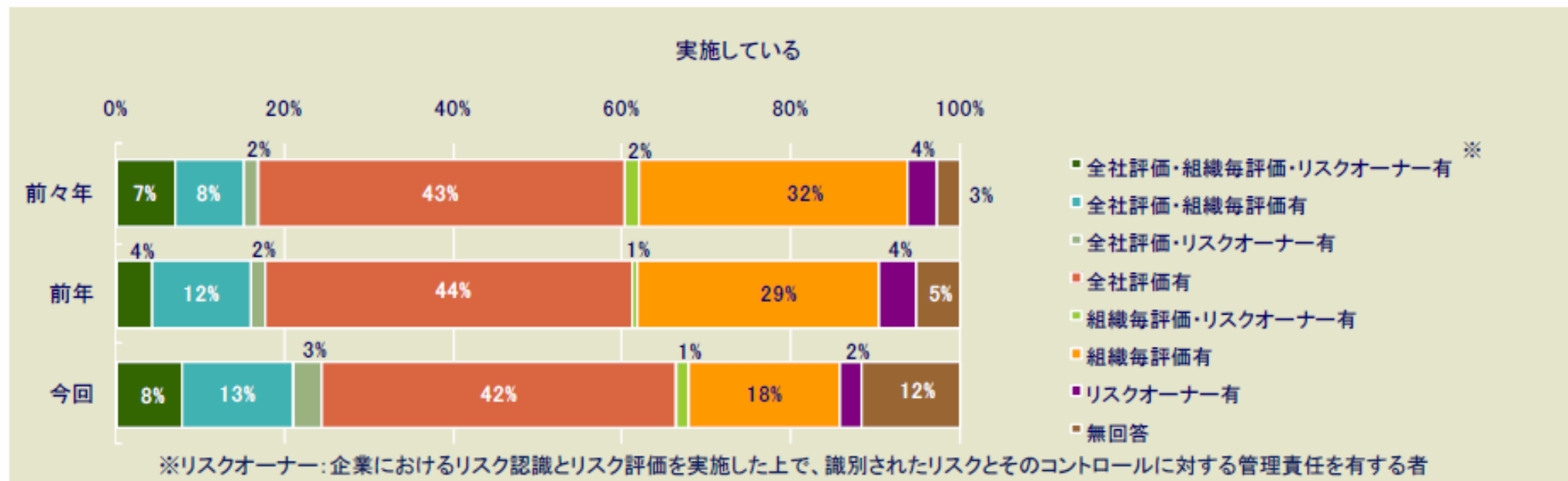
実施している :67% (前年54%、前々年47%)

実施していない:30% (前年42%、前々年50%)

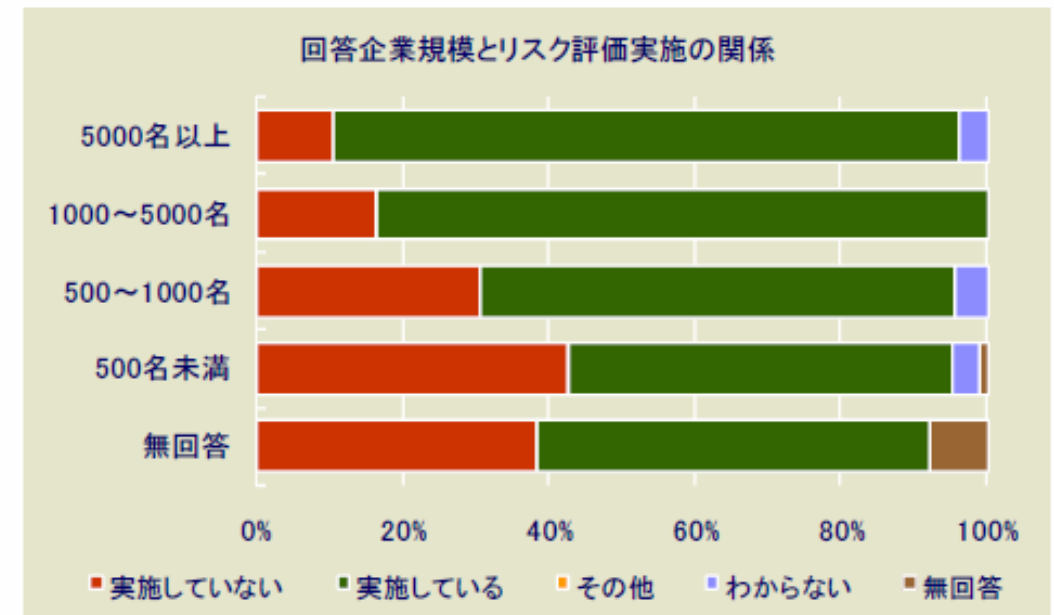
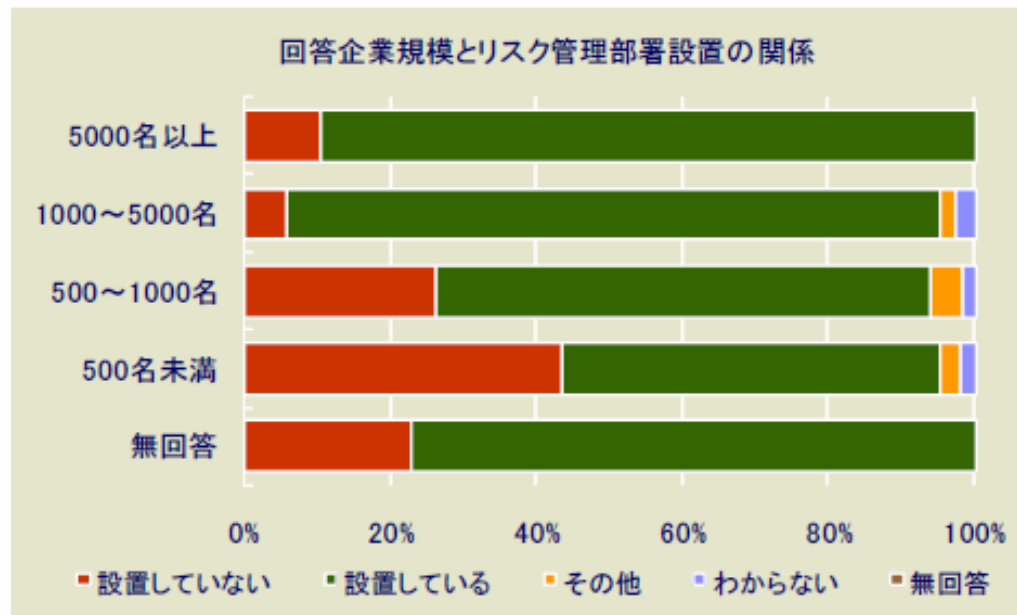
リスク評価に関しては改善傾向を示し、実施していると回答した企業の割合が、2002年の調査開始以来初めて60%を超えた。

実施している企業では、「全社評価」を実施している企業が増加している。内部統制報告制度の影響で、経営者による評価が進められていることが原因の一つとして考えられる。

なお、リスク評価を実施していると回答した企業のうち、財務報告リスクのみを対象としていると回答した企業の割合は20%であった。



2. 企業規模とリスク管理の関係



企業規模とリスク管理部署設置・企業規模とリスク評価実施の関係

リスク管理部署の設置、リスク評価実施は、規模の大きな企業ほど進んでいる傾向が伺える。

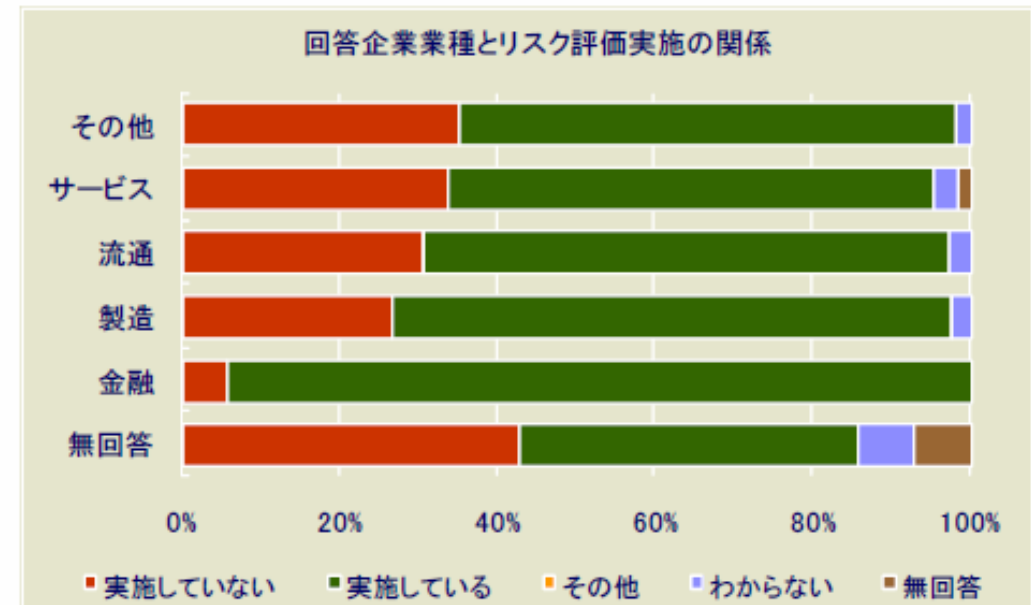
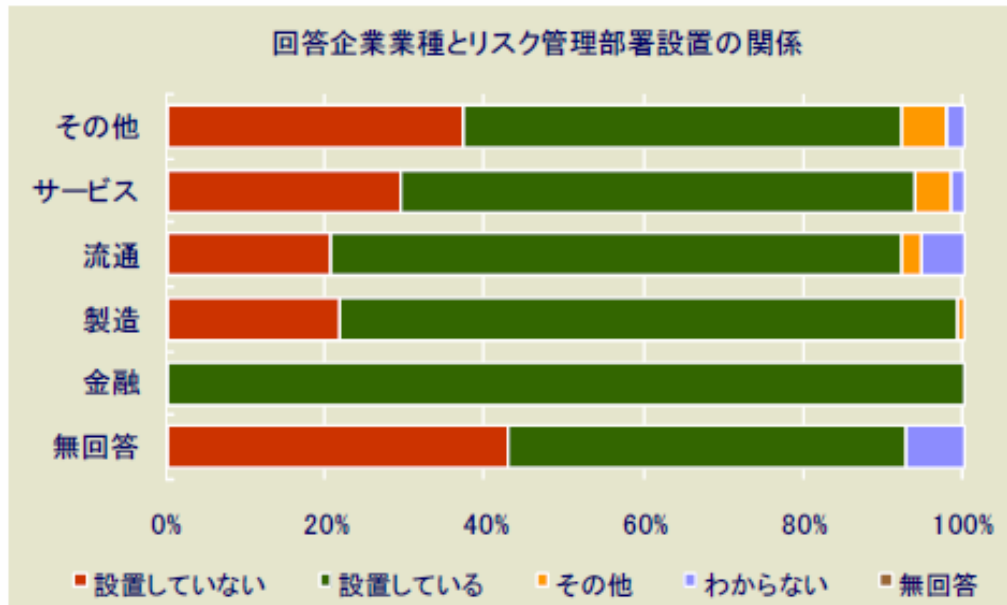
リスク管理部署を「設置している」と回答した企業の割合は、企業規模1000名を境に、規模の大きい企業では増加傾向、規模の小さい企業では減少傾向を示した。

| | | |
|------------------|-------|-------|
| 500名未満の企業： | 前年53% | 今回52% |
| 500～1000名規模の企業： | 前年75% | 今回68% |
| 1000～5000名規模の企業： | 前年81% | 今回89% |
| 5000名以上の企業： | 前年88% | 今回89% |

一方、リスク評価を「実施している」と回答した企業の割合は、全ての規模の企業において増加した。その結果、過去の調査において見られた「リスク評価実施割合がリスク管理部署設置割合に比して小さい」という現象は、どの企業規模においても著しく改善した。

監査法人トーマツ トーマツ企業リスク研究所 『企業リスクマネジメントアンケート調査集計結果』2009年1月8日より

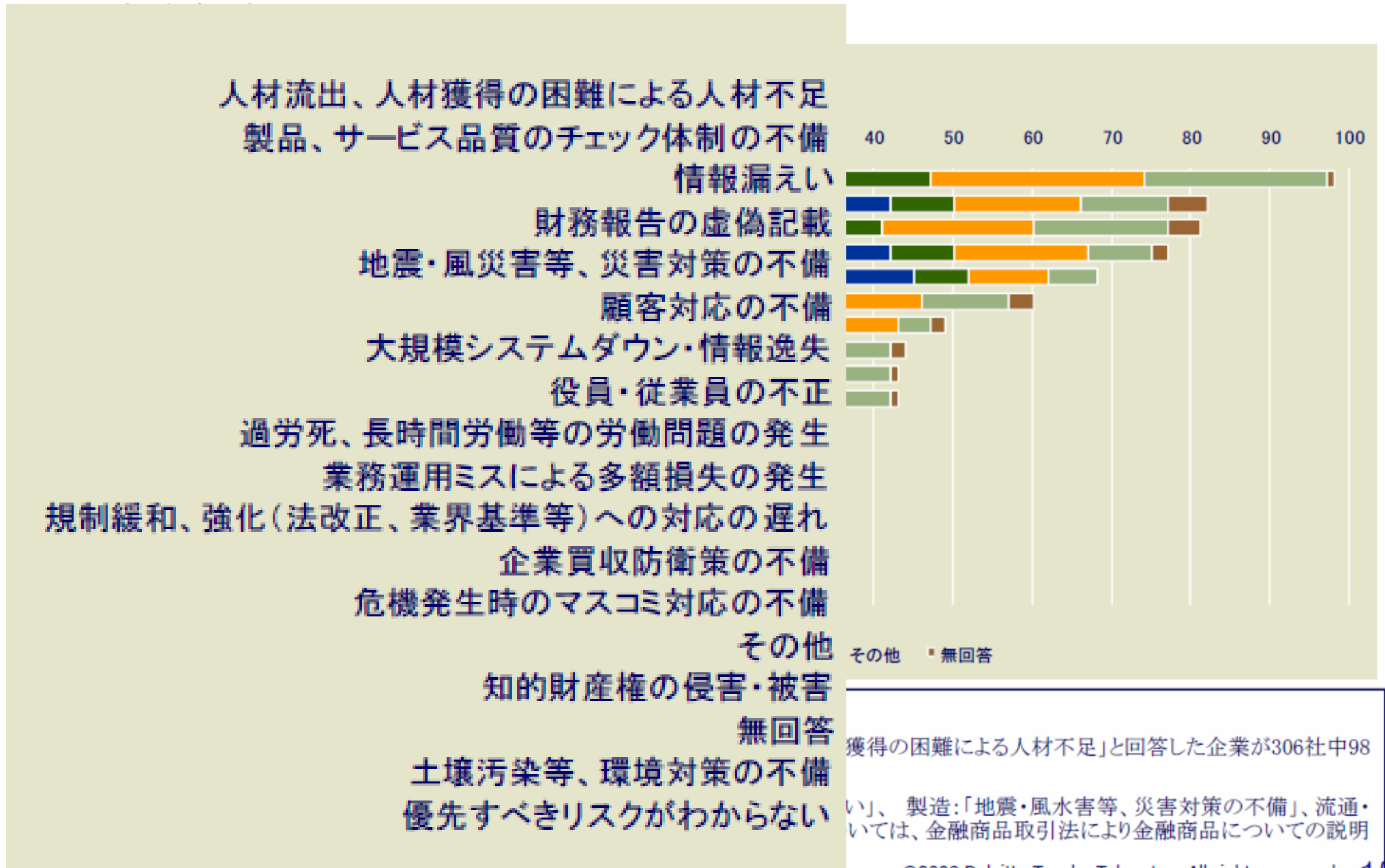
3. 企業業種とリスク管理の関係

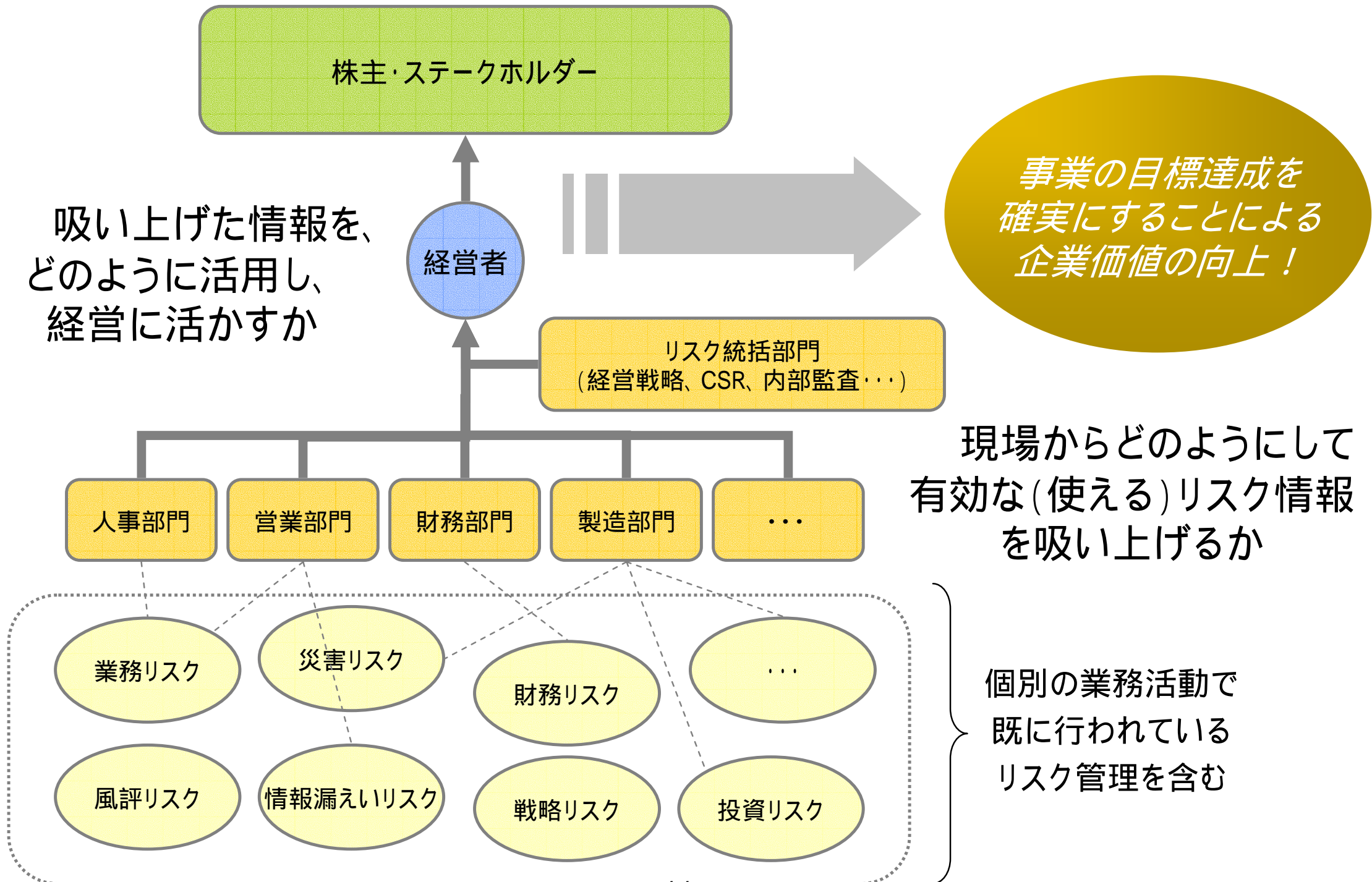


企業業種とリスク管理部署設置・企業業種とリスク評価実施の関係

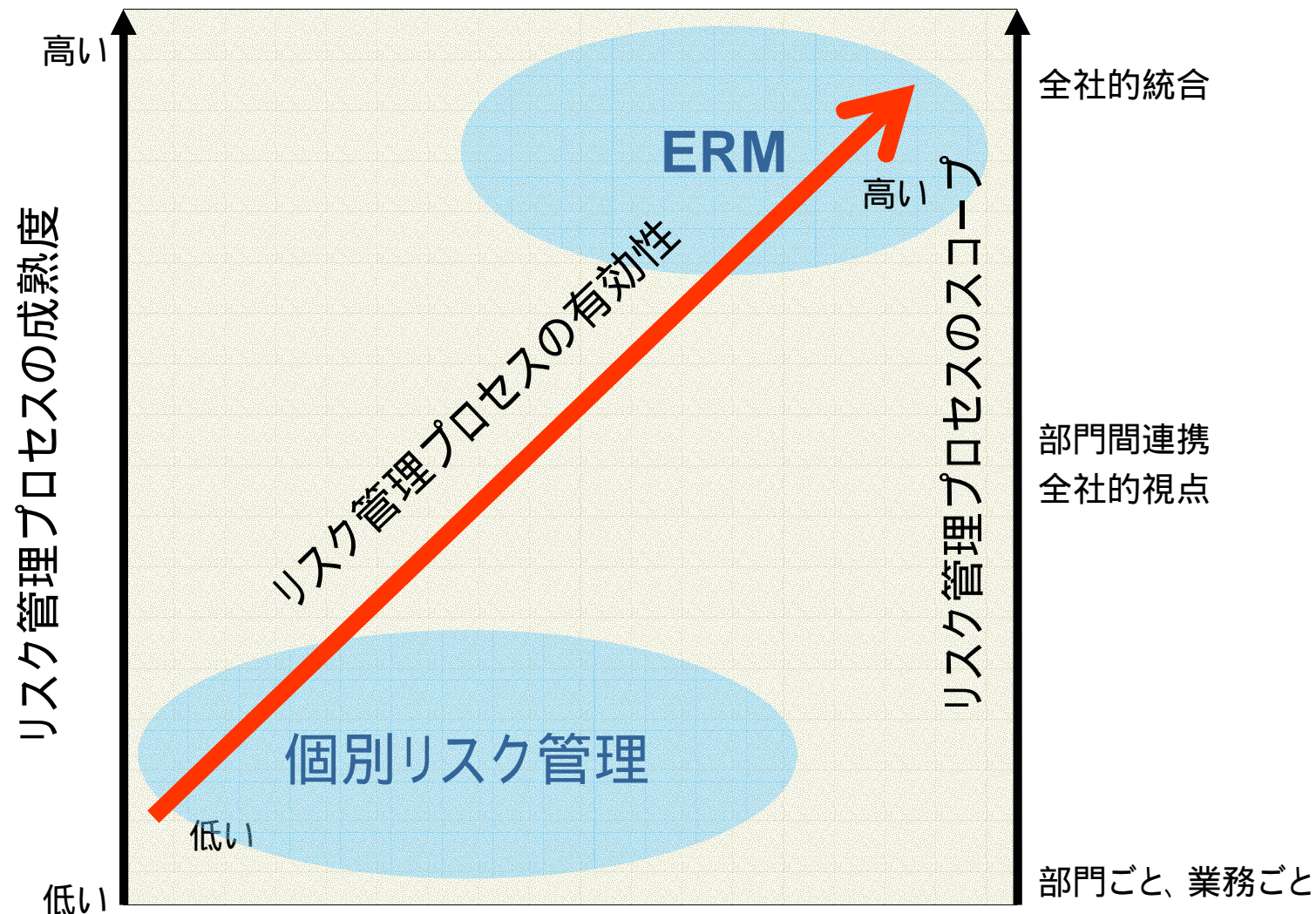
リスク管理部署を「設置している」と回答した企業の割合は、金融業、製造業と流通業において増加し、金融業では設置している割合が100%だった。一方、サービス業で「設置している」と回答した企業は前々年調査から続けて減少傾向にある(前々年：76%、前年：70%、今回：65%)。

リスク評価を「実施している」と回答した企業の割合は、全ての業種で増加している。昨年大幅な伸びを見せた製造業もさらに増加している(前々年：39%、前年：59%、今回：71%)。リスク管理部署の設置割合が減少しているサービス業についても、リスク評価の実施割合は増加している(前々年：52%、前年：49%、今回：62%)。専門のリスク管理部署を設置しないながらもリスク評価は実施する企業が増えていることが伺える。





必ずしもERMを新たな仕組みとして一から立ち上げる必要はなく、個別に行われているリスク管理や、社内に既にある情報を活用し、リスクを統合して管理することにより、リスクマネジメントのプロセスをより有効なものへと成熟させていくことが現実的



社内からのリスク情報の収集

既存のリスクマネジメント活動からのアウトプットや、社内システムにある情報等を活用し、効率的なリスクに関する情報収集が不可欠。

収集した情報の統合

様々なリスクに関する情報を統合し、優先順位付けし、既存のリスクマネジメントに横串を通すことが必要。

リスク情報の可視化

リスク情報を経営に活かすためには、集められた情報から、社内のリスク状況が直感的に把握できることが重要。

リスクの管理(モニタリング)

リスクを取り巻く状況は、日々刻々と変化している。一度情報を集めただけで満足してしまわず、状況の変化に適時に対応できるためのモニタリングを定着させる必要がある。

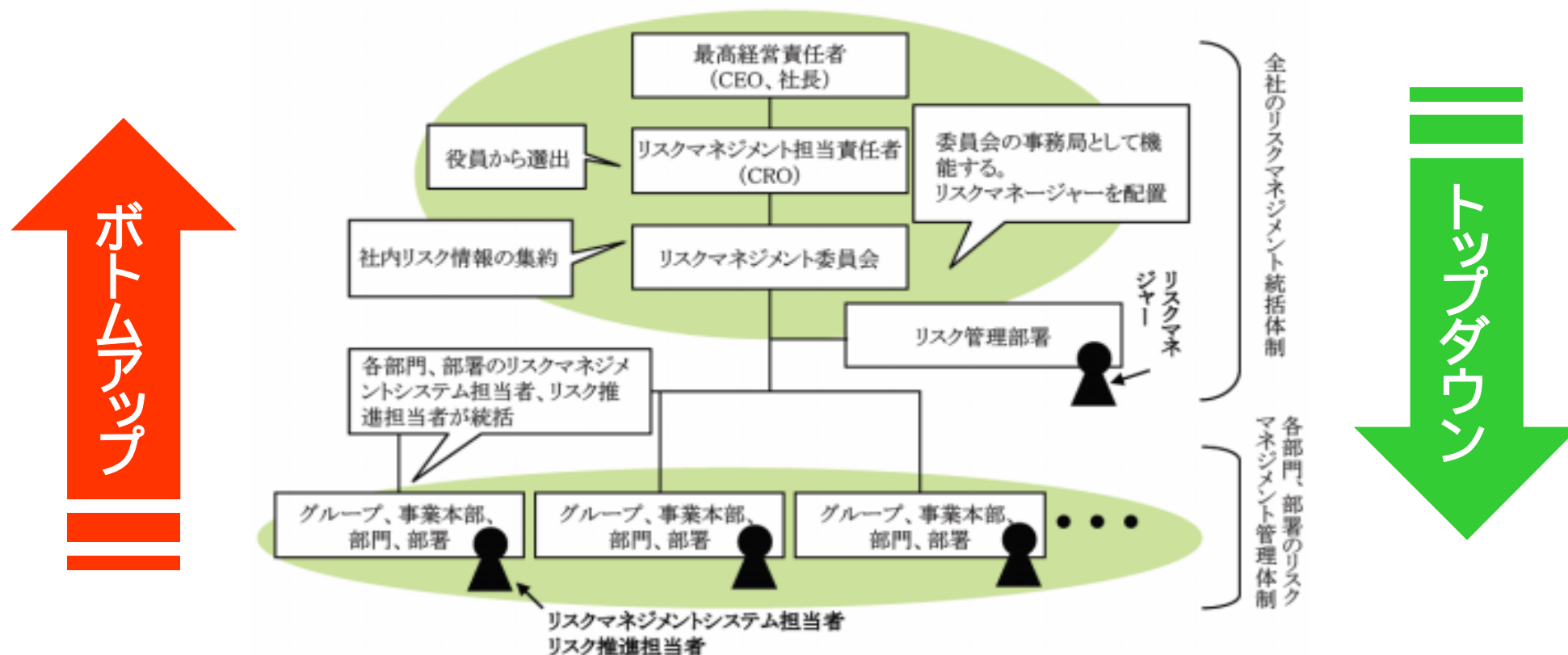
収集

既存のリスクマネジメント活動からのアウトプットや、社内システムにある情報等を活用し、効率的なリスクに関する情報収集が不可欠。

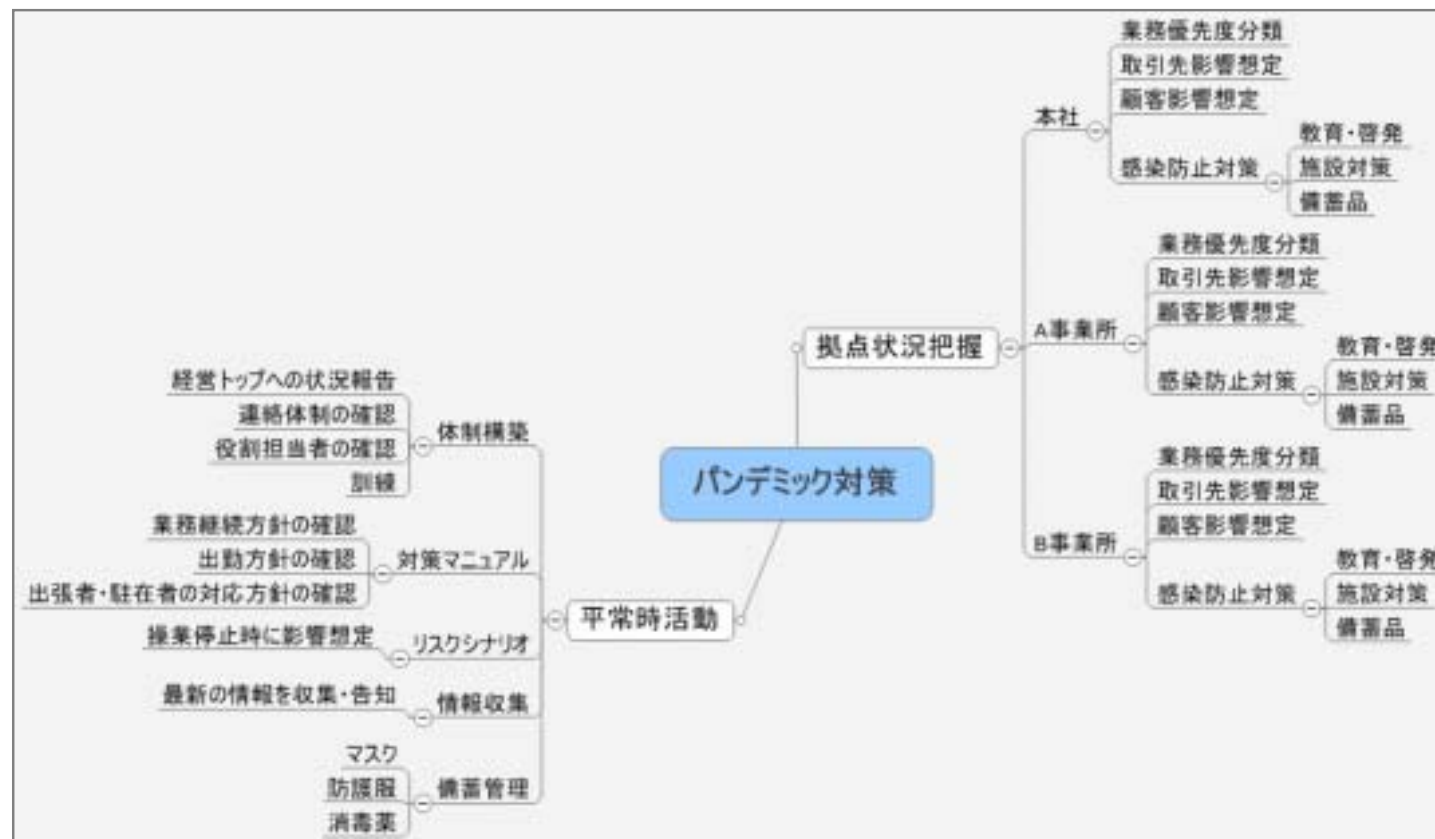
- リスクに関する情報は、既に社内に点在していたり、個別に管理されているものも多いと考えられる
- 既に行われているリスクマネジメント活動があれば、リスクの洗い出し、評価にそこからのアウトプットを活用することで、統合リスクマネジメントの効率化と高度化が図れる
- 社内の情報システムを活用し、リスク情報の収集を効率化



- トップダウンでのリスクの優先順位付けに加え、既存の各業務に組み込まれたリスクマネジメント活動を把握することが必要
- 既に行っている業務活動と重複したリスクマネジメント
日常業務で多忙な現場担当者にとって、時間・工数的な無駄があるばかりでなく、モチベーションを低下させ、リスクマネジメント活動の質の低下をもたらす



- コンプライアンス対応や**BCP**などの活動の中で、リスクマネジメントと共通する情報を活用
 - 情報セキュリティリスク
 - J-SOX**対応のために行った全社統制
 - 事業継続マネジメントのためのビジネスインパクト分析



- リスクの優先順位と性質を踏まえ、以下のような基準を元に事業リスクを測る指標 (**KRI**) を定義

- リスク事象との関連性
- 指標としての客観性
- 定期的な取得可能性
- 指標算出の容易性
- 指標の管理可能性



特にこれらについては、
情報システムを利用した
取得による効果大きい

【KRIの例】

| リスクの顕在化の兆候を表わす指標 | リスクの管理状況を表す指標 |
|--|---|
| <ul style="list-style-type: none">• 事件・事故の件数• 苦情件数• 取引件数、金額• 顧客数• 不正アクセス件数 | <ul style="list-style-type: none">• 業務の担当者数• 担当者一人当たりの業務量• 一人あたりクレーム処理件数• 従業員の同一職務着任期間 |

システムから取得できるリスクに関わるデータの活用例

| | |
|----------|--|
| PC操作 | 注文取消機能の利用時間/回数、クレーム処理画面の表示時間などの端末状況を利用し、リスク関連情報を取得 |
| サーバー操作 | コマンドだけでなく、コマンドを実行した出力結果も保持することで、使用者がどのような情報を見て何をしたかを把握できる。 |
| DBアクセス | 許可されないデータへのアクセス試みや、普段と異なるデータアクセスの兆候などを把握し、リスクの顕在化を防止 |
| プログラム変更 | 許可されないプログラム変更などにより、システムの運用が停止し、業務に多大な影響を与えるリスクを事前に検出し管理 |
| ネットワーク利用 | コンピュータ間の通信をすべて把握し、不正なネットワーク経路を通過したアクセスなどを検出 |

*WEEDS
Windows-Trace*

WEEDS UNIX-Trace

*WEEDS
DB-Trace*

WEEDS ITGC-Trace

*WEEDS
NW-Trace*

統合

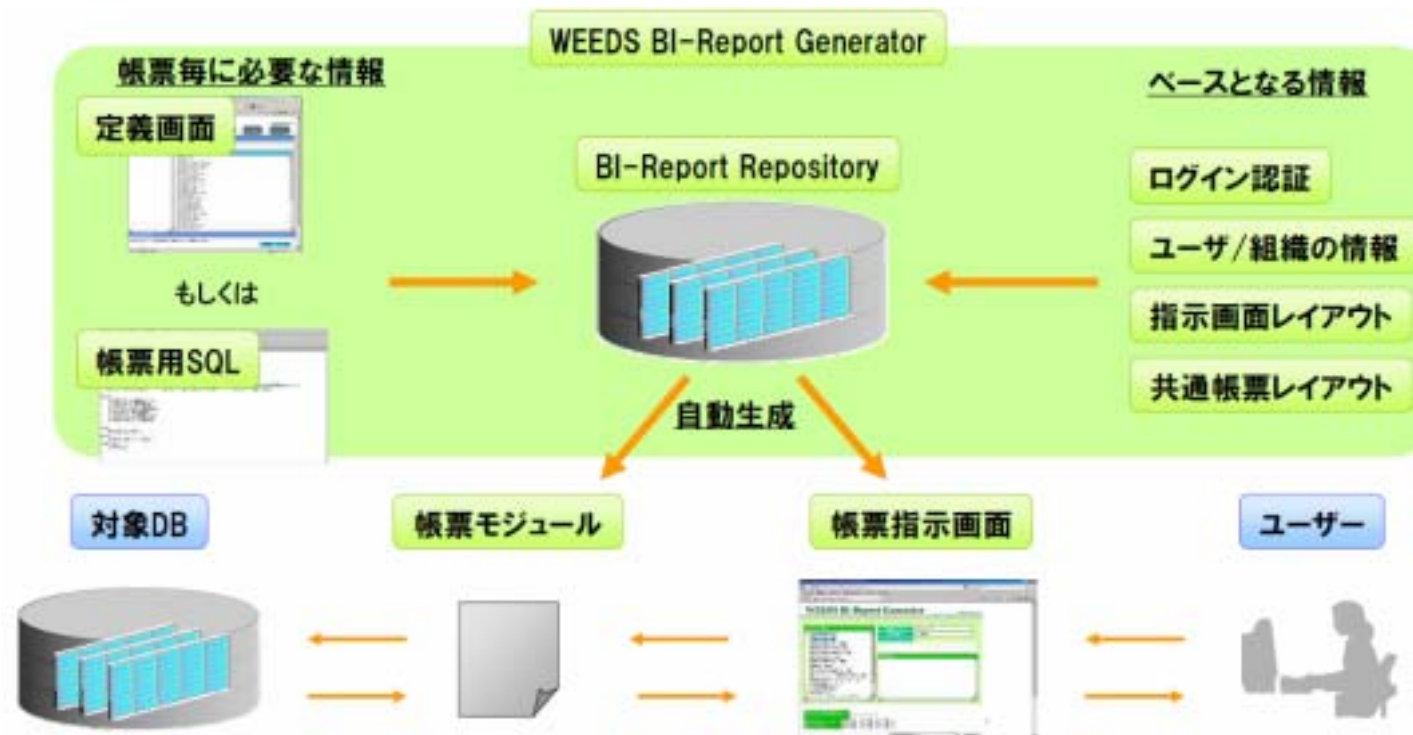
様々なリスクに関する情報を統合し、優先順位付けし、既存のリスクマネジメントに横串を通すことが必要。

- 社内の様々な業務やステークホルダーに関連するリスクを、全社視点から統合
- 集められた情報を元にリスクの所在を明らかにし、対応の優先順位をつける
- いかにデータから意味のある情報を抽出できるかが鍵となる



データ統合の重要性

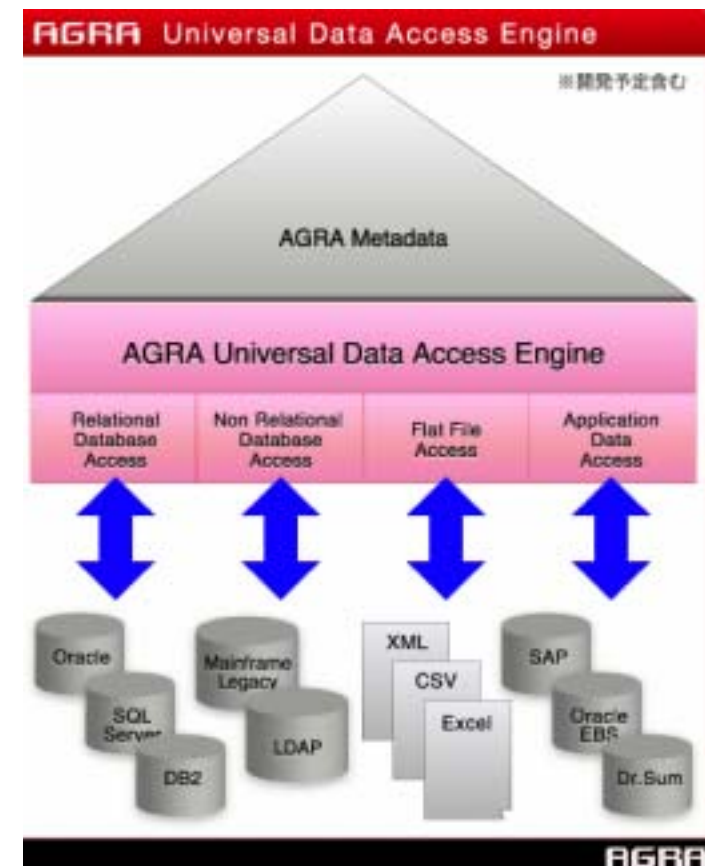
- 全社的なリスク管理は、経営者視点でのリスクの把握と優先順位付けが求められる
- そのためには、個別のリスクに関するデータがばらばらに提供されるのではなく、多忙な経営者に対して必要な情報を効果的に適時に提供できる必要がある
- 均質で確実な情報の提供には、情報システムの活用が必須



コーポレートレポジトリの必要性

- 前述のデータ収集ステップにより、個別の情報は把握できるが、現在の企業のリスク環境は単純ではなく、情報を統合し、そこから意味のあるデータを抽出することが鍵となる
- 企業の歴史と共に、レガシーシステムは複雑化し、リスクに関する情報も複雑なシステム環境の中に埋もれてしまいがち
- 各業務に点在するリスク情報を統合し、全社的なリスク情報のレポジトリを作成することにより、ビジネスの不確実性がより効率的、効果的に管理可能となる

AGRA
Semantic Enterprise Management System

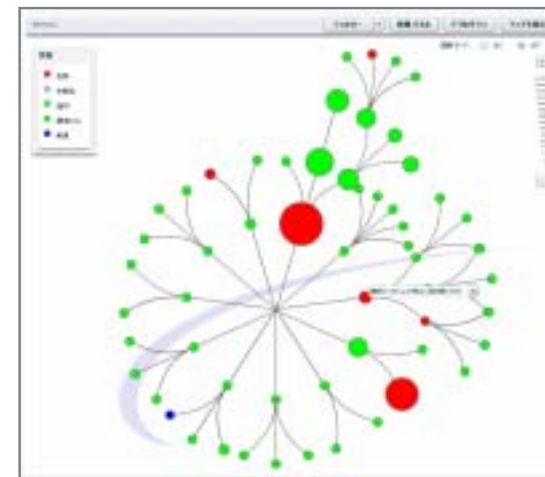
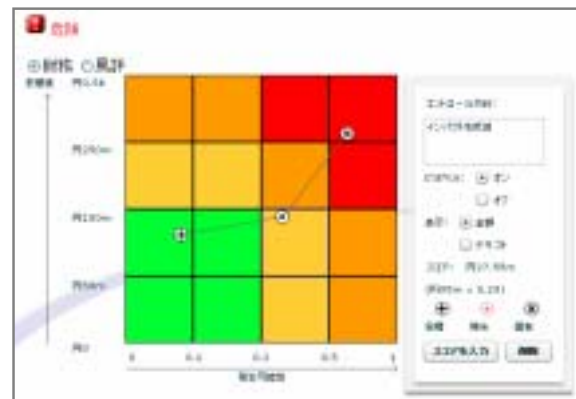


リスク情報の可視化

可視化

リスク情報を経営に活かすためには、集められた情報から、社内のリスク状況が直感的に把握できることが重要。

- リスク情報を経営に活かすためには、最新の情報がいつでもリアルタイムに参照できる必要がある
- 単なる数字の羅列であったり、複数枚のエクセルシートに情報が埋もれてしまっていては、必要なときに必要な判断が下せない
- 直感的にリスク情報を把握できる仕組みが必要



Certus™ Risk は、英国の内部統制を効率的かつ効果的に導入するために**2000年**に開発され、英国で高い評価を受けているソフトウェアです

- ビジネスのパフォーマンスを脅かすリスクやコンプライアンス問題の対応状況をリアルタイムで**視覚的に**把握できる、**Webベースのアプリケーション・ソフトウェア**です
- リスクやコントロールの担当者やリスクプロフェッショナルは、シンプルでわかりやすいインターフェースを使って、**リスクの情報を簡単にアップデート**できます
- 組織のトップやマネジメントは、イントラネットやブラウザを使用していつでも**組織全体の状況を視覚的に**把握し、情報を**さまざまな角度から分析**できます

全社のリスクを
リアルタイムに可視化！



コーポレート・ガバナンス

パフォーマンスとリスクのレポート ↑ ↓ 経営上のアドバイスと指示

certus
RISK



Certus™ Risk(旧製品名Acertus Governance)は、英国では**2000年**からの実績があり、ストラテジック・リスク誌主催の**2007年ヨーロッパ・リスクマネジメント・アワード**において、今年度の**最優秀リスクマネジメント製品**に選ばれました。

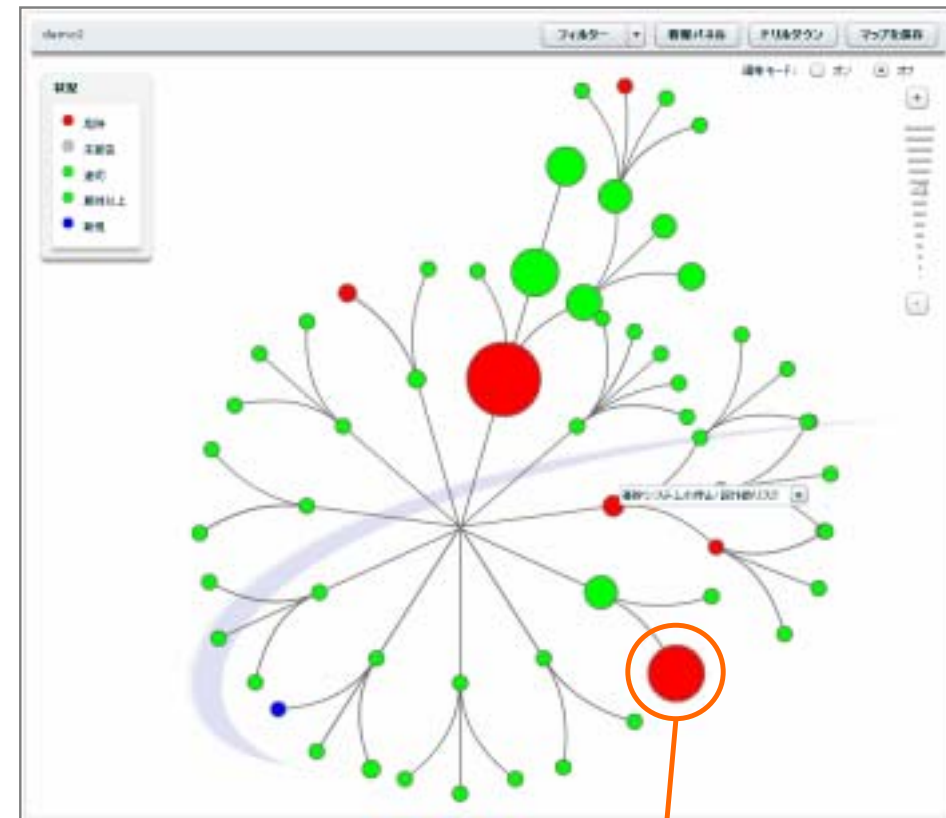
2007 Strategic RISK
EUROPEAN RISK MANAGEMENT
AWARDS



リスク階層の可視化

丸の大きさと色によって、リスクの状況を一目で把握

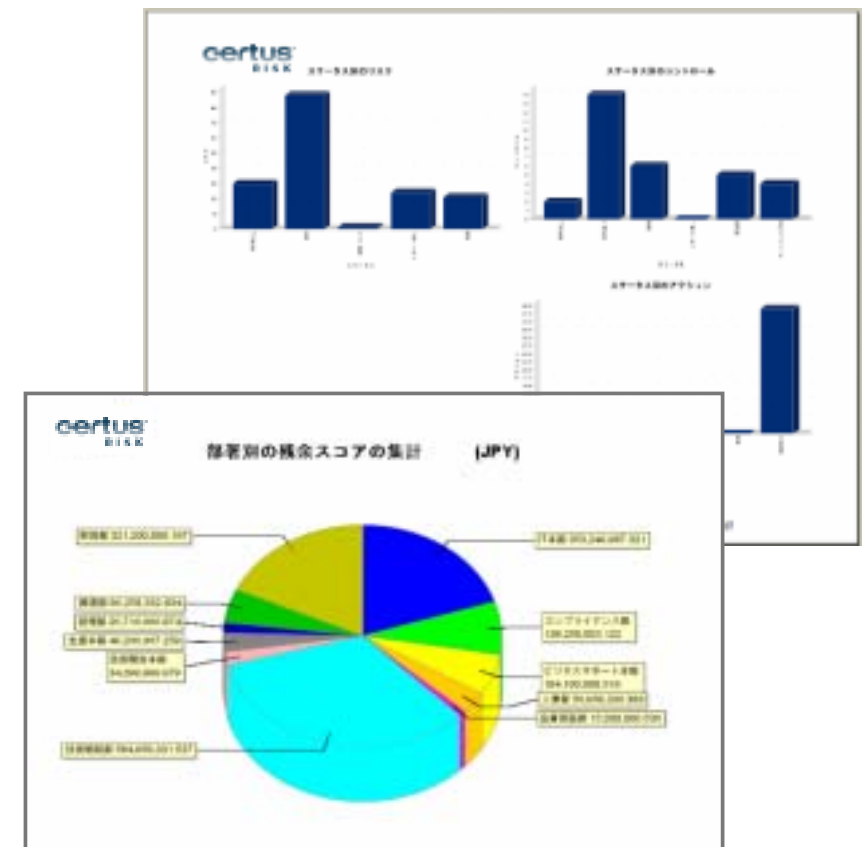
- **Certus Risk**では、リスクのレポート階層を、独自のインタラクティブなグラフィックツールであるデータマップを使用して表現します。
- マップの中の 一つ一つが、リスクとして定義されています。
- 組織の中の全てのリスクの情報を、階層的に視覚化して、わかりやすく表示します。
- マップ上では、リスクの詳細を表示したり、属性でリスクをフィルターしたり、リスクの階層構造をドリルダウンしたりできます。



一つ一つの がリスク

報告のためのデータ集計・分析が容易に可能

- すべてのレポート機能においてデータへのセキュリティ・アクセス制御が利用可能
- **PDF、Excel、およびWord形式へのワンクリックのデータエクスポート**
- **30種類以上の定型レポート**
- 追加のレポート要件対応をサポートする、ユーザによるカスタマイズが可能な「ビュー・ビルダー」
- カスタムレポート

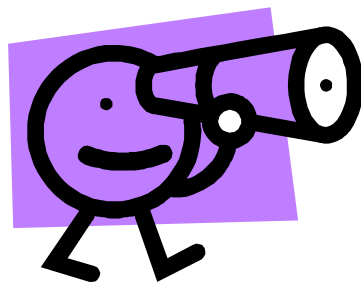


リスクの管理 (モニタリング)

管理

リスクを取り巻く状況は、日々刻々と変化している。一度情報を集めたただけで満足してしまわず、状況の変化に適時に対応できるためのモニタリングを定着させる必要がある。

- リスク情報は一度収集しただけでは意味がなく、洗い出されたリスクが適切に継続的に管理できる仕組みが重要
- そのためには、各リスクとそのコントロールに責任を持つ担当者を明確にすることが必要
- 担当者からのリスク状況の報告は、通常業務への負担にならない形で、かつ確実に集められなければならない
- ITを活用したリスクモニタリングの仕組みが必須



Certus™ Riskは、リスク担当者にとってのリスクの報告をシンプルで容易にするとともに、マネジメントにとって必要なリスクの情報を適時に可視化できるツールです。

組織のトップやリスク管理者にとっては...

Certus™ Riskの可視化機能により、イントラネットでブラウザを使用していなくても組織全体のリスクの状況を視覚的に把握し、情報をさまざまな角度から分析できる、**リスクの可視化ツール**です。

リスク担当者にとっては...

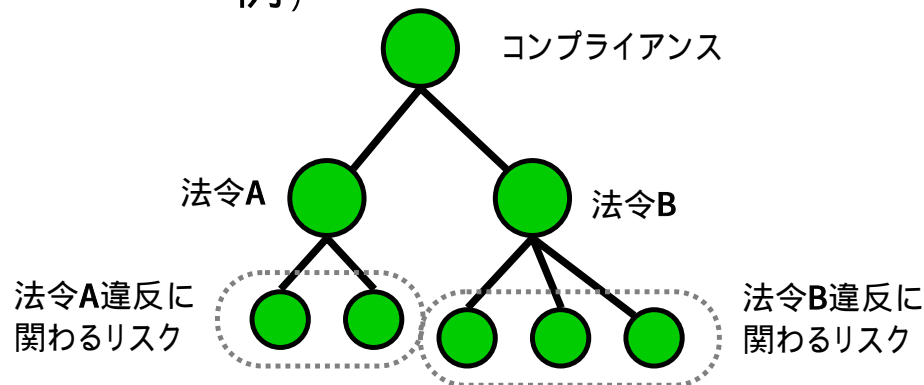
ビジネスを日常的に行っていく中で、顕在化する可能性のある様々なリスクと、それに対して適切に対応していくためのアクション、コントロールを一箇所で管理し、シンプルでわかりやすいブラウザベースのインターフェースを使って情報を簡単に更新し、状況を報告できる**リスク報告ツール**です。

リスクの階層化とリスク担当者

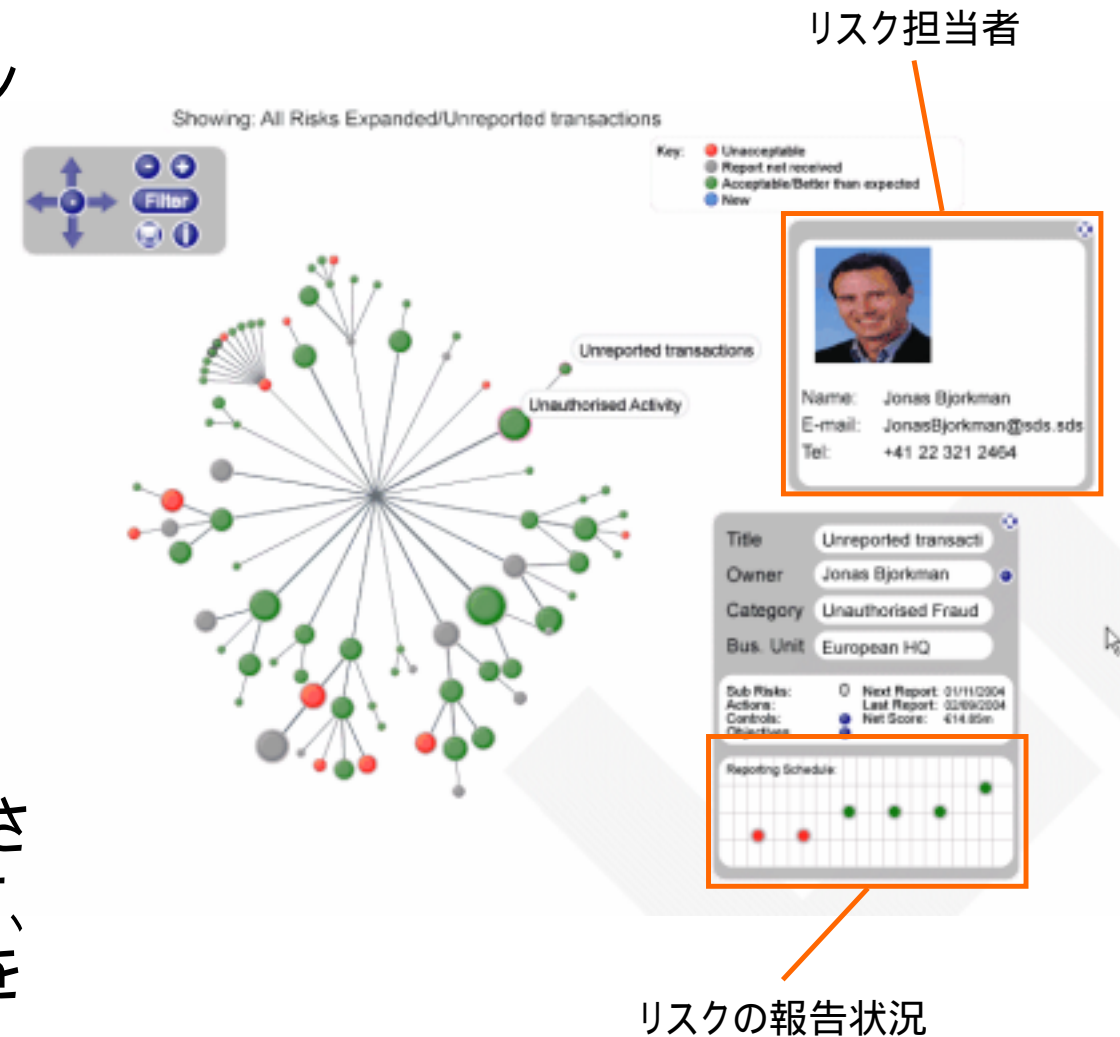
各リスクに担当者が設定され、Web上で定期的に報告

- 各リスクは、リスクのレポートラインに合わせて階層化されます

例)



- 各リスクには担当者が設定され、リスク担当者は、各リスクに設定されたリスクの報告期間に合わせて、Web上で定期的にリスクの状況を報告します



Showing: All Risks Expanded/Unreported transactions

Key:
● Unacceptable
● Report not received
● Acceptable/Better than expected
● New

Unreported transactions
 Unauthorised Activity

リスク担当者

Name: Jonas Bjorkman
 E-mail: JonasBjorkman@sds.sds
 Tel: +41 22 321 2454

Title: Unreported transacti
 Owner: Jonas Bjorkman
 Category: Unauthorised Fraud
 Bus. Unit: European HQ

Sub Risks:
 Actions:
 Controls:
 Objections:

Next Report: 01/11/2004
 Last Report: 02/09/2004
 Net Score: 414.85e

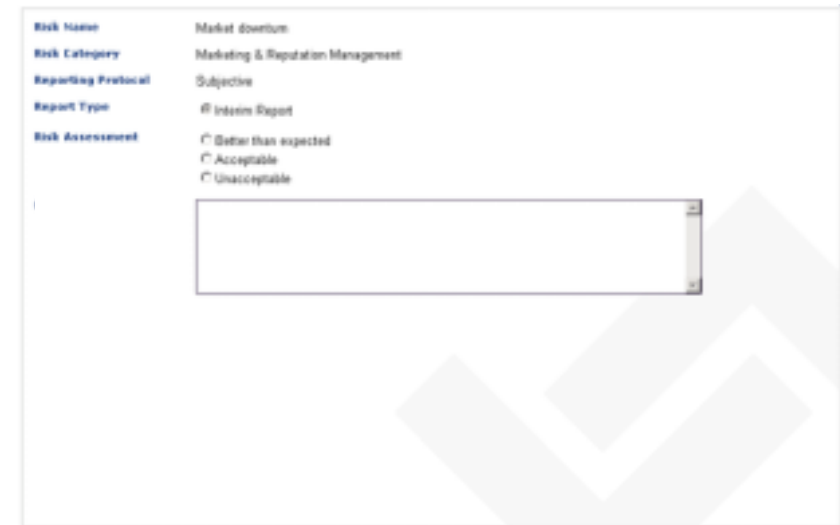
Reporting Schedule:

リスクの報告状況

リスクの状況報告

担当者に負荷をかけない簡単な報告方法とメールによる通知

- 担当者は、報告期日が近づくとメールで通知を受け取り、システムにログインし報告します。
- 「主観的評価」方法では、リスク報告の際、現在のリスク状況を主観的に次の3つから選択します：
 - 期待以上
 - 適切
 - 危険
- 「数値評価」方法では、リスク報告の際、リスクの状況を示す指標となる数値(%、個数、日数等 = KRI)を入力します。数値が期待以上だと になり、期待以下だと になります。
- 指定期間内に担当者からの報告がない場合には、リスクの色が になります
- リスクが または になると、親リスクの担当者に通知メールが送られます。



This screenshot shows the 'Subjective Evaluation' reporting form. The fields are as follows:

- Risk Name: Market downturn
- Risk Category: Marketing & Reputation Management
- Reporting Protocol: Subjective
- Report Type: Interim Report
- Risk Assessment:
 - Better than expected
 - Acceptable
 - Unacceptable

There is a large empty text area at the bottom for comments.



This screenshot shows the 'Numerical Evaluation' reporting form. The fields are as follows:

- Risk Name: Market downturn
- Risk Category: Marketing & Reputation Management
- Reporting Protocol: Numeric
- Report Type: Interim Report
- Assessment Value: 83
- Infation: Inflation

There is a large empty text area at the bottom for comments.



Certus Risk デモ



ご清聴、誠にありがとうございました。

Certus™ Riskや弊社サービスに関するお問い合わせは、
GRCジャパン株式会社
阪田 麻紀
TEL: 03-3597-0033
Mail: maki.sakata@grc-j.com
www.grc-j.com