Powerful Insights.
Proven Delivery.®

第188回CFOセミナー（東京）
第189回CFOセミナー（大阪）

SOX対応の成熟化と経営に資する次世代内部統制への展望

～2012年ポストSOXサーベイの調査結果を踏まえて～

東京会場（7月18日）
大阪会場（7月19日）

プロティビティLLC

protiviti®
Risk & Business Consulting.
Internal Audit.

Agenda

- はじめに
- Post SOX Survey 調査結果
  - SOXがもたらす効果
  - SOX対応プロセスの現状と効率化
  - SOXと不正対応
  - CAATの活用
- COSO内部統制フレームワークの改訂
- ガバナンス・リスク・コンプライアンス（GRC）への取り組み
- おわりに

protiviti

はじめに

日本で内部統制報告制度が適用されてから5年、米国で、サーベンス・オクスレー法404条が適用されてから10年

- **適用初年度は、財務・経理部を超えて内部統制プロジェクト対応に多くの企業が苦労した。**
- **その後数年でさまざまな工夫が行われ、内部統制評価の方法は成熟化し、対応コストも低減されてきた。**
- **海外では内部統制整備の活動はその後、ガバナンス・リスク・コンプライアンス（GRC）へと拡大・進展している。**

日本CFO協会及びプロティビティで共催した、“Post SOX Survey～SOXからGRC（ガバナンス・リスク・コンプライアンス）へのトレンド調査～”

- **日本企業の現状の取組状況や抱えている課題**
- **従来の内部統制への取り組みをさらに効率化し、企業価値の最大化に資するGRC体制構築への展開への留意点**

・本資料では、我が国の内部統制報告制度および米国サーベンス・オクスレー法404条の要請、つまり、財務報告に係る内部統制の経営者による整備運用評価および外部監査人による監査を総称して“SOX”としている。

Post SOX Survey

～ SOXからGRC（ガバナンス・リスク・コンプライアンス）へのトレンド調査 ～

調査結果

2012年ポストSOXサーベイの調査の概要

（調査概要）

- ✓ 日本CFO協会、プロティビティの共催
- ✓ ネットでの回答（弊社TSA）及び紙（ファックス）による回答
- ✓ 有効回答数　175名

（プロファイル）

✓ 企業規模	グループ売上高1兆円以上	20%
	5000億円以上1兆円未満	18%
	1000億円以上5000億円未満	27%
✓ SOX適用属性	J-SOX適用上場会社（親会社）	74%
✓ 回答者役職	役員・部長	39%
	マネージャー	41%

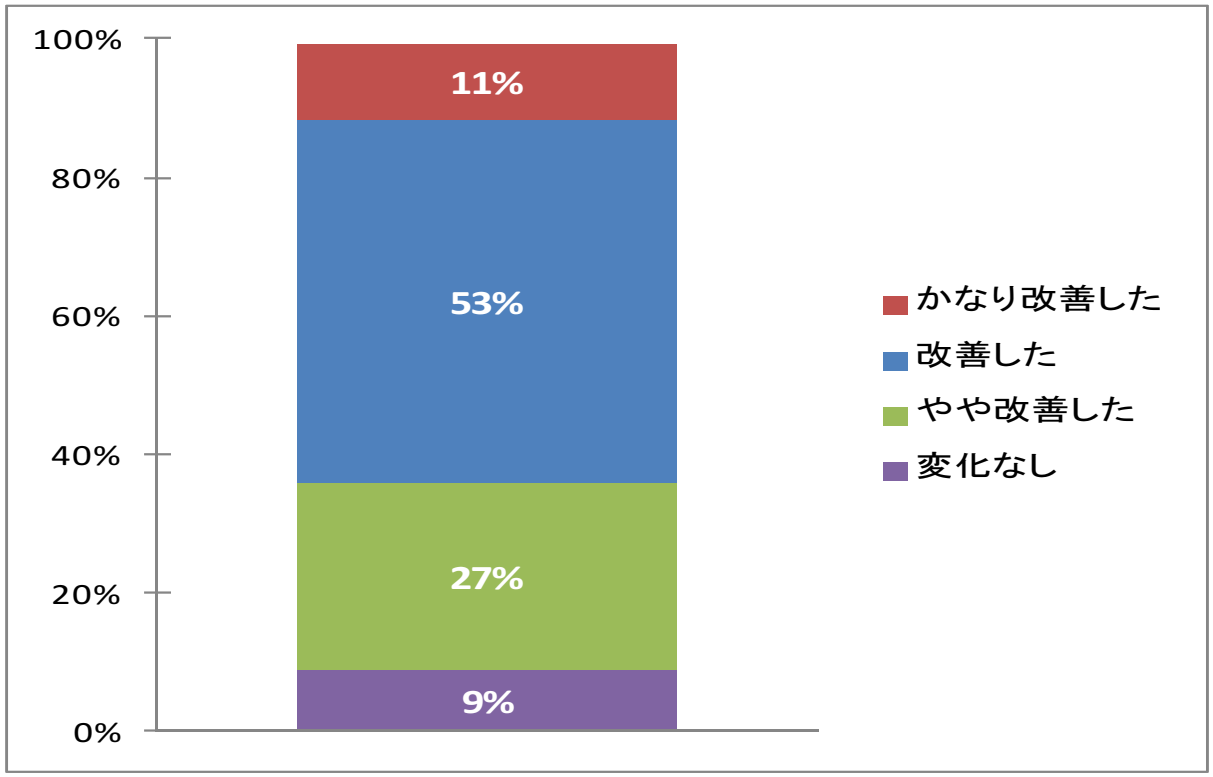
Post SOX Survey 調査結果

～ SOXがもたらす効果 ～

SOXがもたらす効果
～財務報告の内部統制が改善

90%以上の会社は、日米のSOX法制度の施行以来、財務報告に係る内部統制が改善。

SOX対応を経て、財務報告に係る内部統制に改善があったか



我が国の内部統制報告制度の動き

● 内部統制報告制度の状況　（施行から４年目）

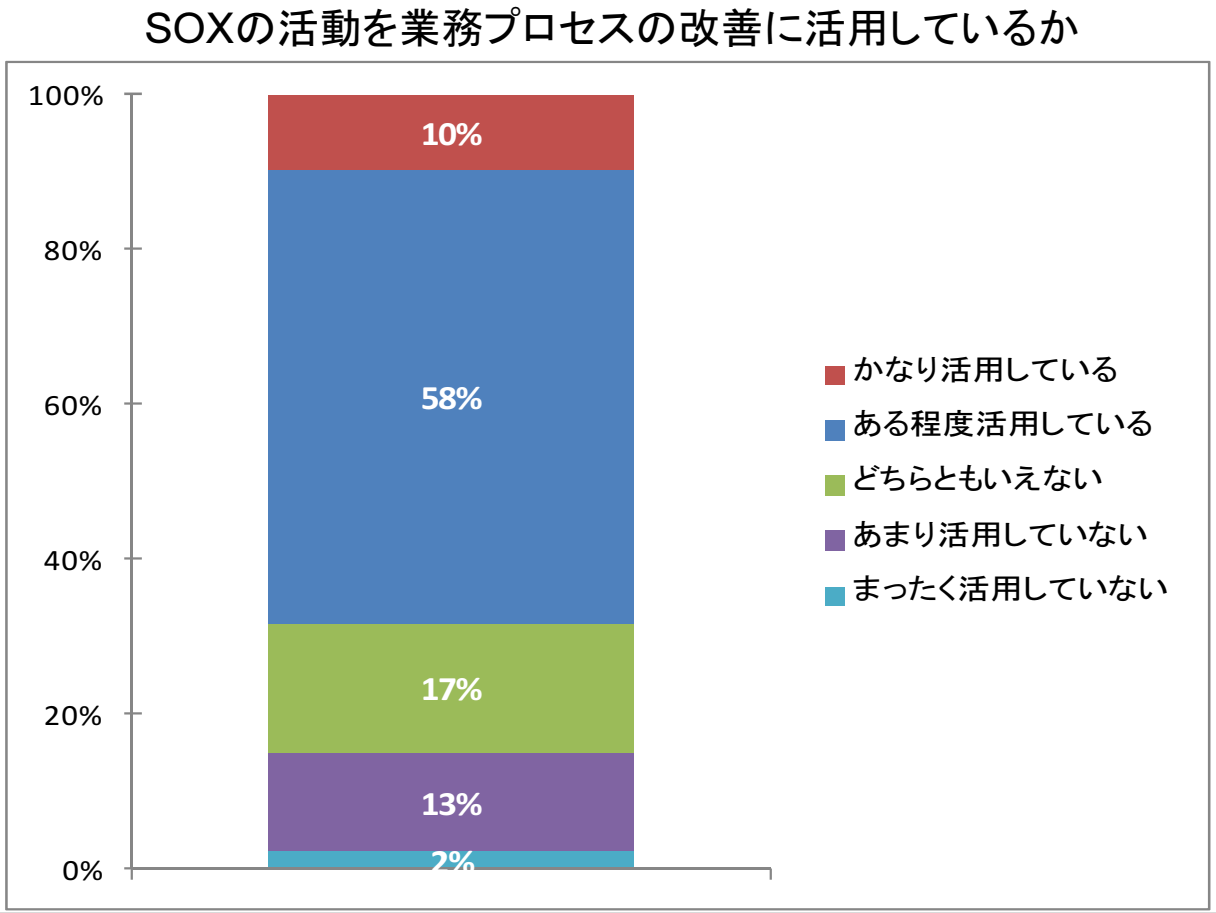
ー年々訂正内部統制報告書での不備報告が増加
ー有価証券報告書の訂正も行っているケースが大半

報告種別 ＼ 適用年度	初年度 2009年6月 ～2010年5月	2年目 2010年6月 ～2011年5月	3年目 2011年6月 ～2012年5月	4年目 2012年6月 ～2013年5月
内部統制報告書 重要な不備	92	34	16	**22件**
訂正内部統制報告書 (”有効”⇒”不備”のケース)	8 （8社）	16 （11社）	27 （15社）	**50件** **（20社）**

【“開示すべき重要な不備”の件数　　適用年度別1年間】
*期間は報告書の提出日を基準

SOXがもたらす効果
～業務プロセスの改善

70%近くの会社は、SOXの活動を業務プロセス改善に活用。



protiviti

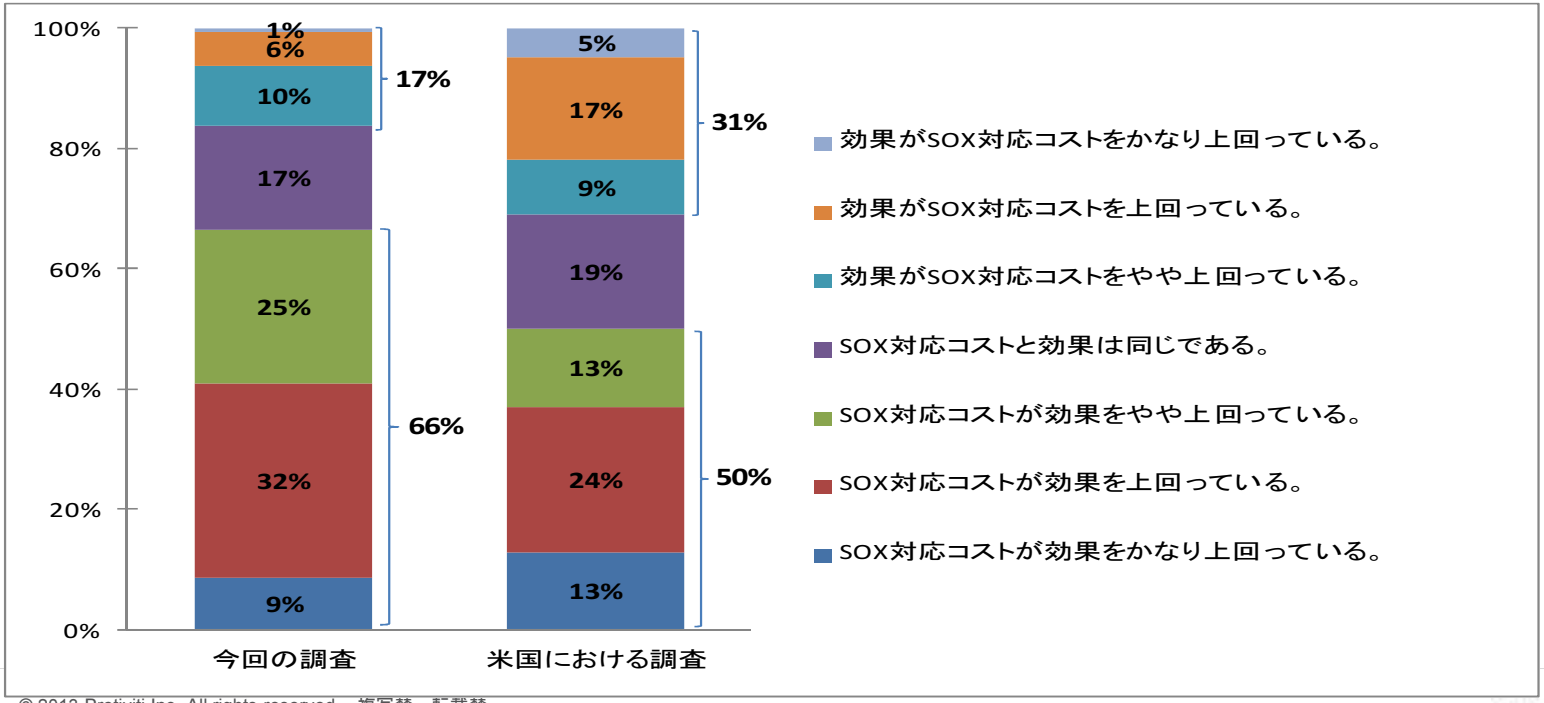
SOXがもたらす効果
～費用対効果

66%:コスト ＞ 効果
17%:効果　＞ コスト

50%:コスト＞ 効果
31%:効果 ＞ コスト

- 米国企業では、SOX対応を効率化し、コストを削減し、コンプライアンス向上、業務プロセス改善に活用し、効果を増大。
- 日本企業では、今後、SOX対応を、内部統制の改善、業務プロセスのさらなる改革に積極的につなげていくことが、コストを上回る効果を得るカギになるのではないか。

SOX対応に関する費用対効果についてどのように捉えているか

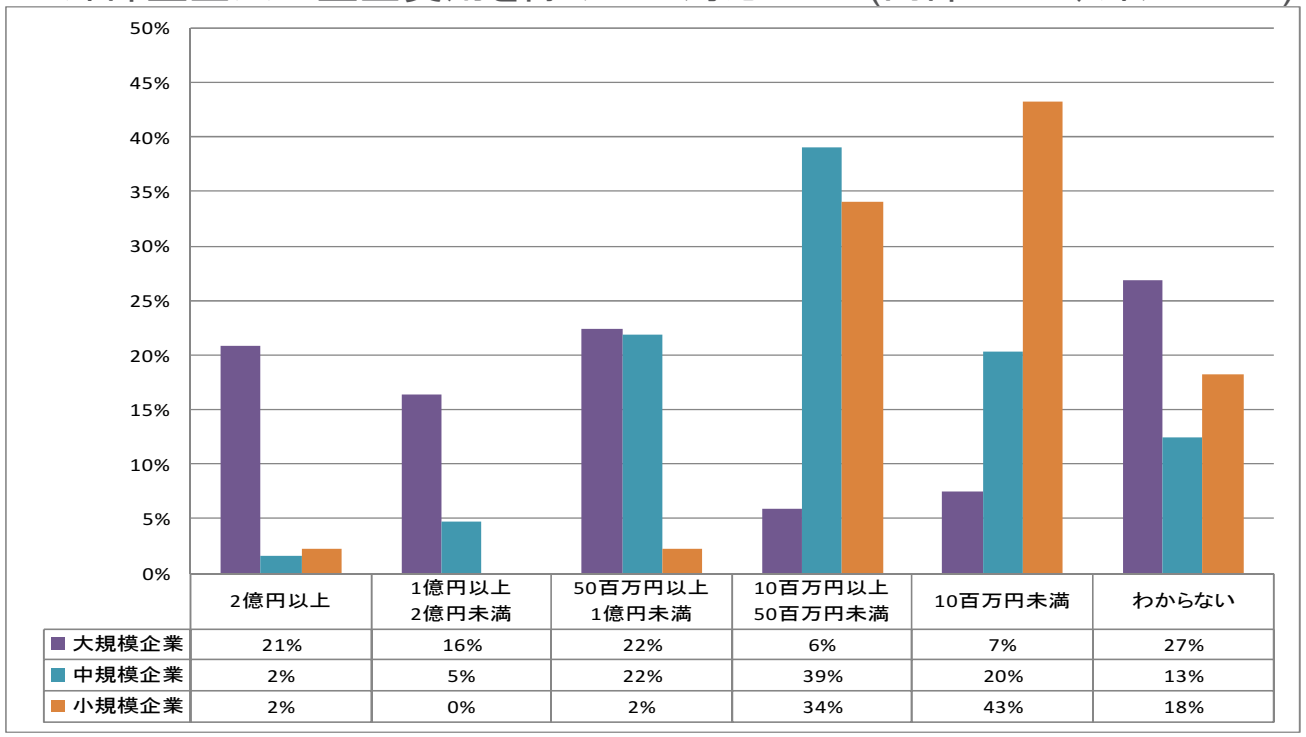


protiviti

SOXがもたらす効果
～SOX対応コスト

- 大規模企業は1億円以上が36%、小規模企業は5千万円未満が77%と、SOX対応コストは企業規模と相関している。
- 「わからない」という回答が相当割合存在。
  - ➢ 費用対効果を検証する点からもSOXコストの適時・適切な把握が必要

外部監査人の監査費用を除くSOX対応コスト(内部コスト、外注コスト)はどのくらいか



	2億円以上	1億円以上 2億円未満	50百万円以上 1億円未満	10百万円以上 50百万円未満	10百万円未満	わからない
大規模企業	21%	16%	22%	6%	7%	27%
中規模企業	2%	5%	22%	39%	20%	13%
小規模企業	2%	0%	2%	34%	43%	18%

【大規模企業】
売上高5,000億円以上
【中規模企業】
売上高500億円以上
5,000億円未満
【小規模企業】
売上高500億円未満

protiviti

Post SOX Survey 調査結果

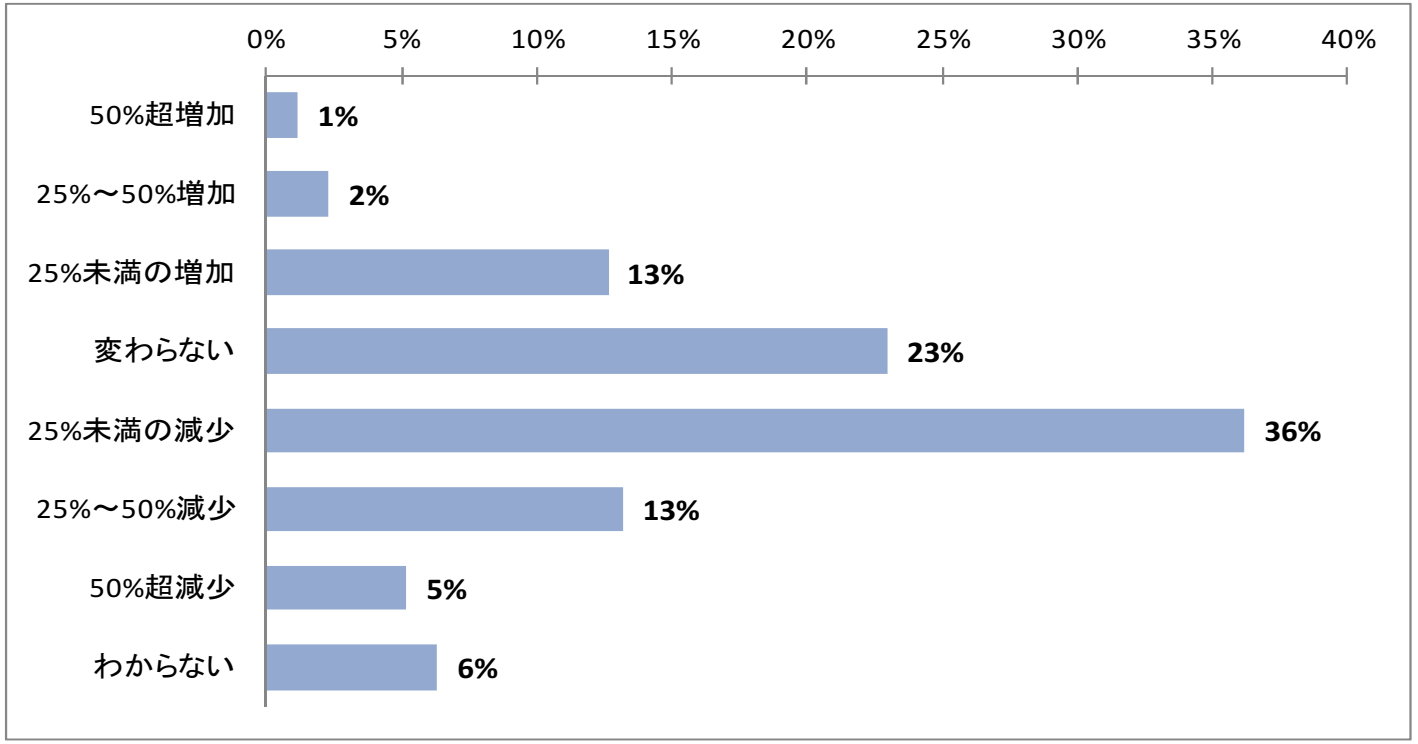
～ SOX対応プロセスの現状と効率化 ～

SOX対応プロセスの現状と効率化
～評価対象コントロールの増減

過半数の企業が評価対象コントロールを減らしている。

→今後規制対応と会社独自の取り組みを分けて、各々の対応方針を明確にした上で、活動を推進していくことも重要ではないか。

全社的な内部統制（組織レベル統制）を除き、評価対象としたコントロールは初年度対応に比べどのぐらい増減したか

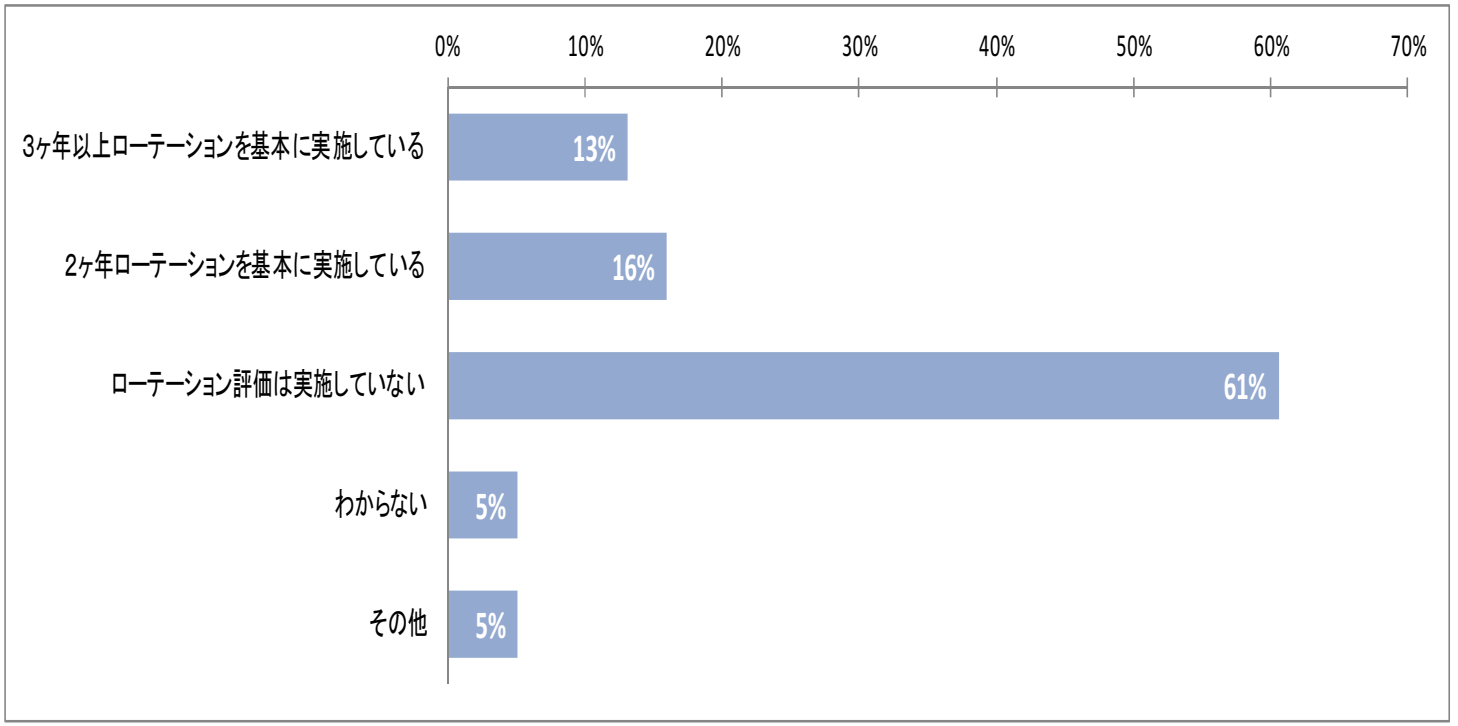


protiviti

SOX対応プロセスの現状と効率化
～評価対象拠点のローテーション

- 拠点ローテーションを実施している企業は30%弱。
- 拠点ローテーションを実施していない企業が61%で、検討の余地ありか。

業務プロセスに係る内部統制の評価について、
評価対象拠点のローテーション評価を実施しているか

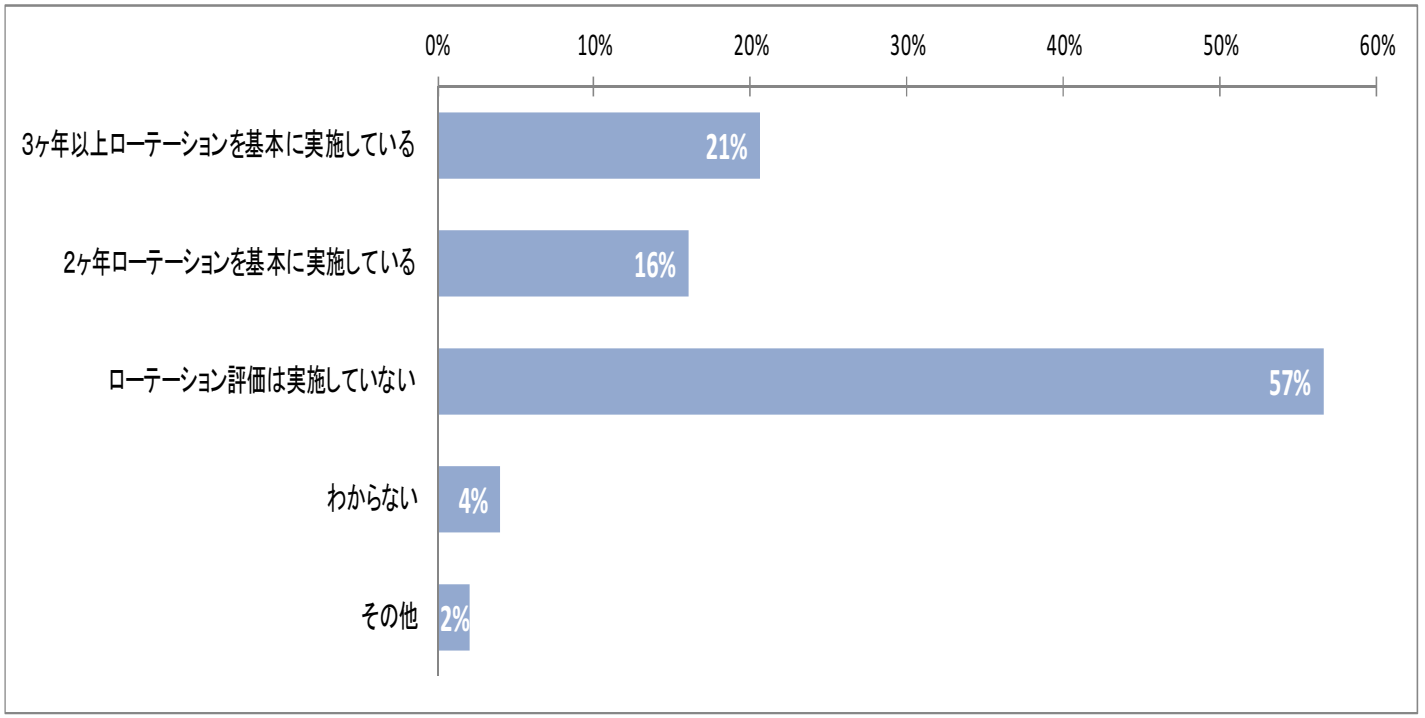


protiviti

SOX対応プロセスの現状と効率化
～評価対象拠点のローテーション

- プロセスローテーションを実施している企業は37%
- プロセスローテーションを実施していない企業が57%
  - ローテーション評価が有効なケースもありうるのでは。

業務プロセスに係る内部統制の評価について、
業務プロセスのローテーション評価を行っているか



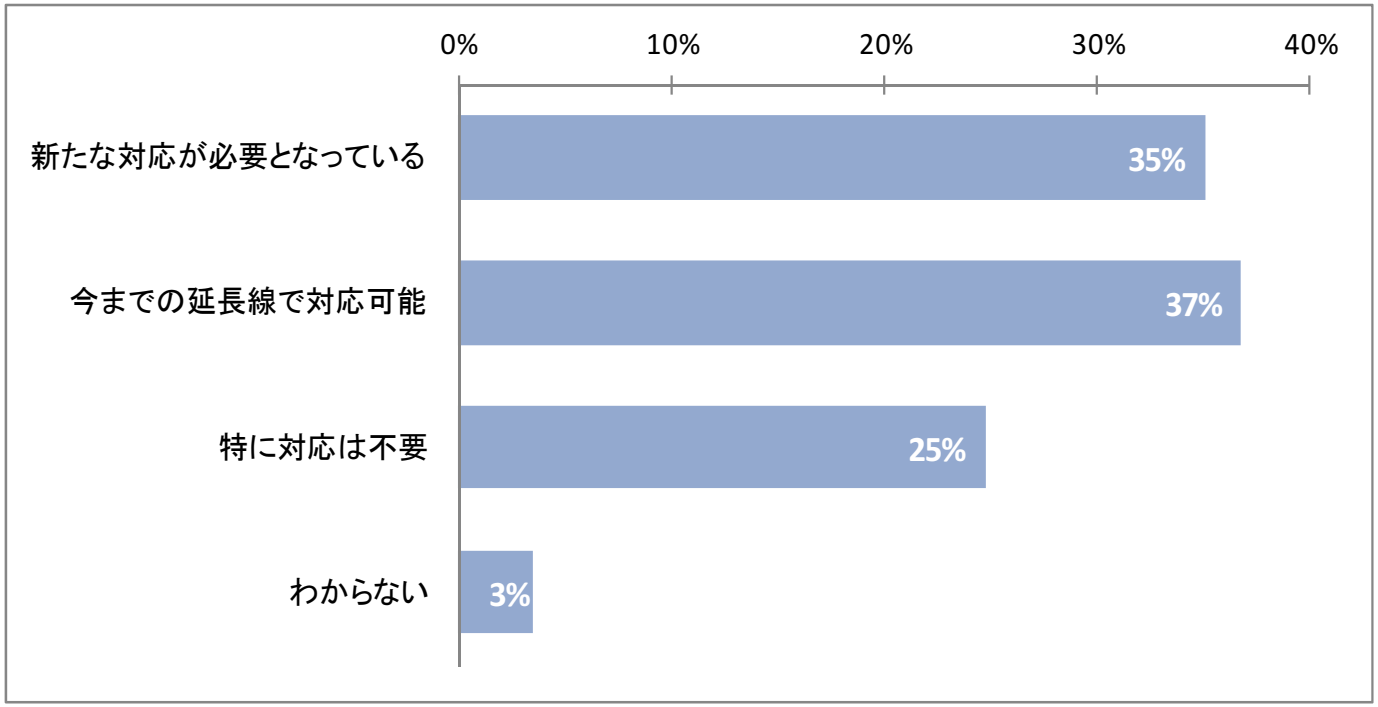
protiviti

SOX対応プロセスの現状と効率化 ～海外拠点対応

35%の企業が、今後新たな対応が必要と回答。

→ グローバル化に伴い、内部統制の取組み範囲が広がり、取組み方法についても工夫が必要となっている。

グローバル化の進展に伴い、海外拠点対応が課題となっているか



protiviti

Post SOX Survey 調査結果

～ SOXと不正対応 ～

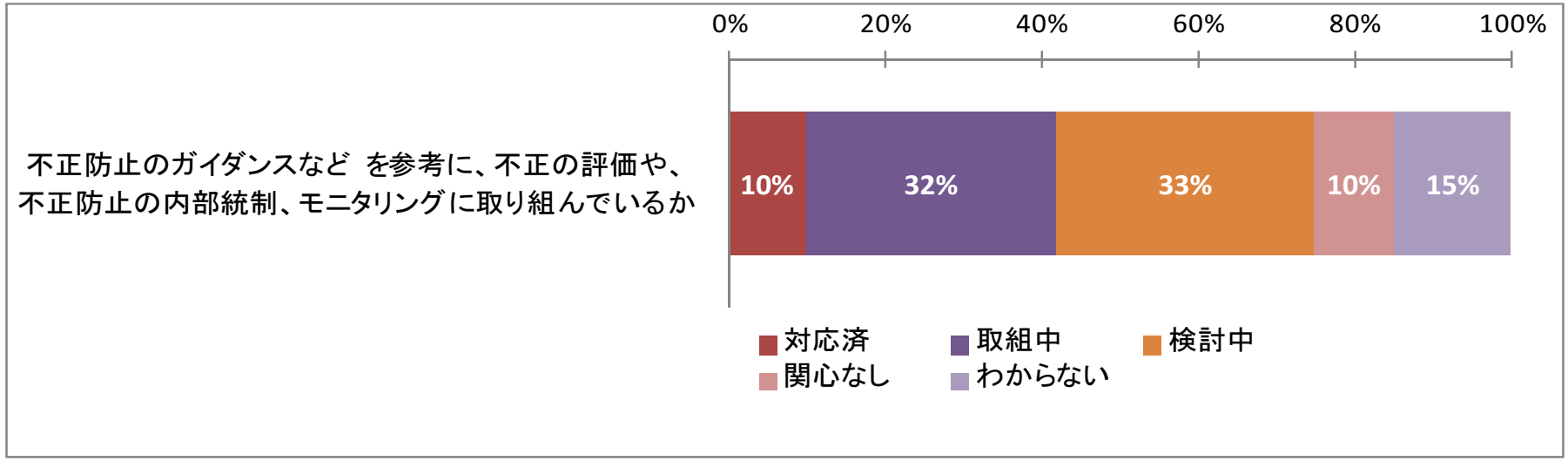
SOXと不正対応
～不正への取り組み（1）

- 不正への対応は、対応済・取組中とする回答は40%強にとどまるが、検討中という回答を合わせると、70%以上の企業が何らかの対策が必要と回答

不祥事が発覚すれば、実際の損失のみならず、株価下落、格付け低下、ブランドイメージ毀損のおそれ

不正は複雑なものも増えており、従来の対応では不十分

→不正に焦点を当てた活動が求められる



protiviti

SOXと不正対応
～不正への取り組み（2）
会計監査のあり方

監査における不正リスク対応基準の骨子は、以下の通りである。

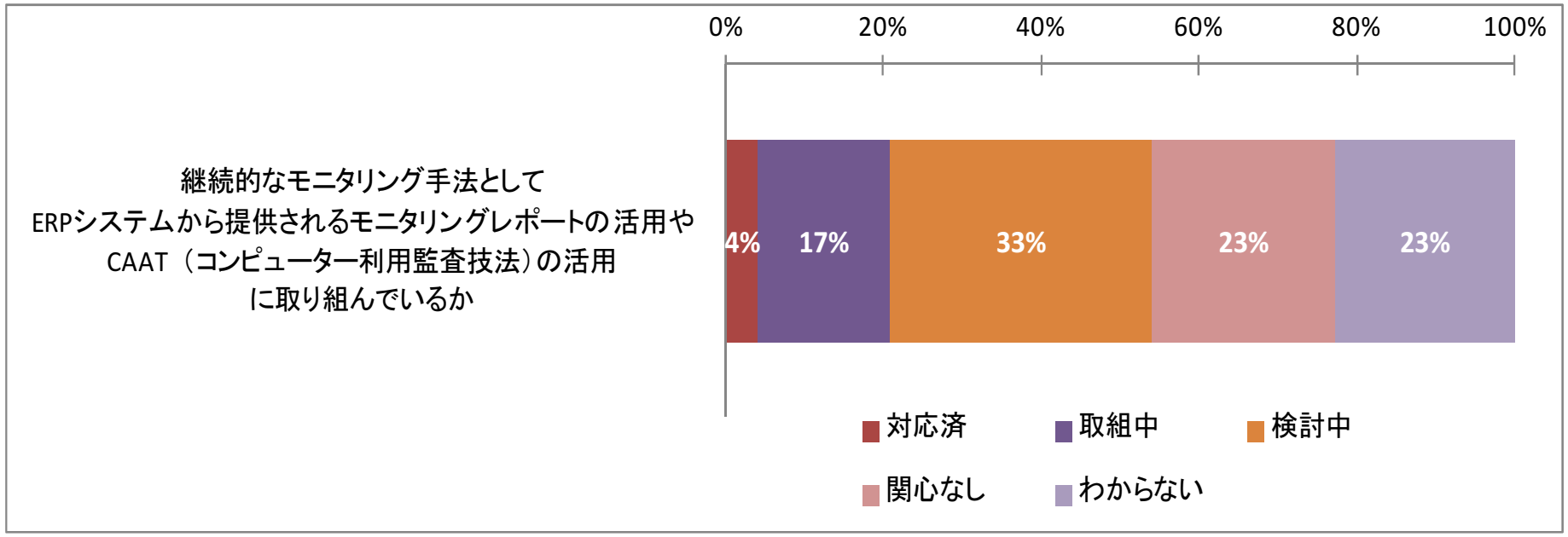
#	項目	内容
1	適用範囲等	✓金融商品取引法に基づき開示を行っている企業に対する監査 ✓平成26年3月期決算に係る財務諸表監査から実施
2	責任主体	✓不正に関しては、一義的には財務諸表作成者である経営者の責任 ✓ 企業におけるコーポレート・ガバナンスのあり方の検討をなどを含め、幅広い観点からの取り組みが重要
3	監査人のリスク評価	✓ 虚偽表示のリスクの評価に当たっては、企業の内部統制の整備状況等が重要な要素 ✓ 内部統制の取り組みを考慮するともに、取締役の職務の遂行を監査する監査役等と適切に連携を図ること
4	循環取引	✓ 循環取引など、取引先と通謀がある場合、取引先監査人との連携が有用であるが、解決すべき論点が多いことから、除外
5	不正を示す状況	✓「不正の端緒」の「徹底調査」 ⇒「不正による重要な虚偽の表示を示唆する状況」に対して「追加的な監査手続きを実施」

Post SOX Survey 調査結果

～ CAATの活用 ～

CAATの活用
～モニタリングレポート、コンピュータ利用監査技法

- 対応済・取組中とする回答が21%にとどまるも、検討中との回答を加えると過半数に及ぶことから、モニタリングレポート・CAAT（コンピュータ利用監査技法）への関心は高い。
  - モニタリングレポート・CAATを活用により、取引全体・データ全体（ビッグデータ）を対象とした、網羅的かつ効率的な検証、不正の兆候の発見が可能となるため、今後取り組む企業が増えていくものと思われる。



protiviti

CAATの活用
～データ分析ツール

CAAT(Computer Assisted Audit Techniques)とはコンピュータ支援監査技法のことを指します。ツール(コンピュータ)を利用することでデータ分析、データ監査、継続監査などの実施に役立てることが出来ます。

内部監査の専門職的実施の国際基準

「内部監査人は、テクノロジー・ベースの監査技法とその他のデータ分析技法の使用を考慮しなければならない」

データ分析ツール（CAAT）

セキュリティ分析ツール

(ex. 職務分掌の設定のチェックなど)

- Assure Security
- Approva
- Logical Apps

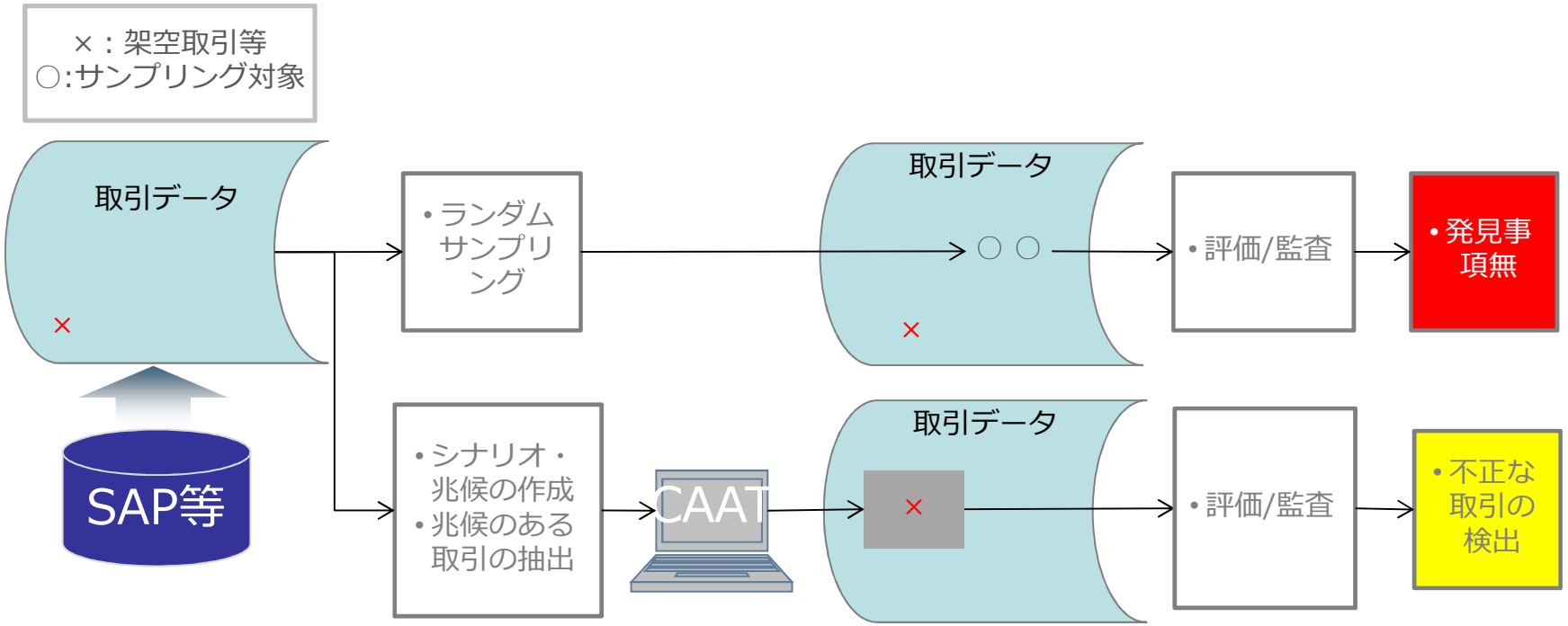
データ分析ソフトウェア

(ex. 不正な経費申請のチェックなど)

- IDEA
- ACL
- SPEND RISK

CAATの活用
～不正対応　テスト対象の抽出　高度化のケース

ＣＡＡＴの活用により、母集団全体から不正の兆候を有する取引等を抽出し、
不正な取引を検出する能力を高めることができます。



メリット

- 母集団すべてを対象として、サンプリングによる抜け落ちのリスクを低減させることが可能
- 不正を発見できる可能性が高まること

protiviti

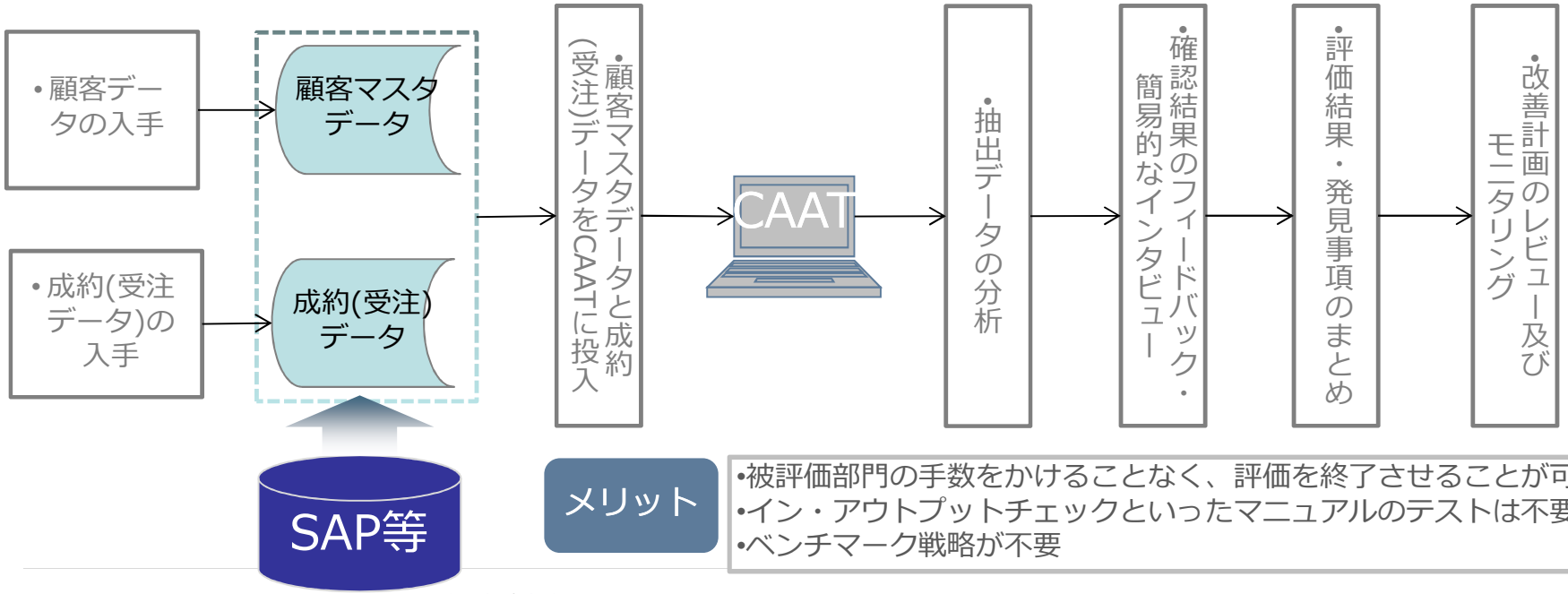
CAATの活用
～テスト対象の自動化　効率化のケース

IT業務処理の業務(例:インプットコントロール等)において、
CAAT を活用することで評価の効率化が可能となります。

インプット（入力）コントロール

（コントロールの内容）
販売管理システムに、契約を登録する場合、予め取引先マスタに登録された顧客だけしか選択することができない
（テストの目的）
顧客マスタに登録されていない得意先が、成約（受注）データファイルに存在していないことを確かめる。

評価実施部門



メリット

- 被評価部門の手数をかけることなく、評価を終了させることが可能
- イン・アウトプットチェックといったマニュアルのテストは不要
- ベンチマーク戦略が不要

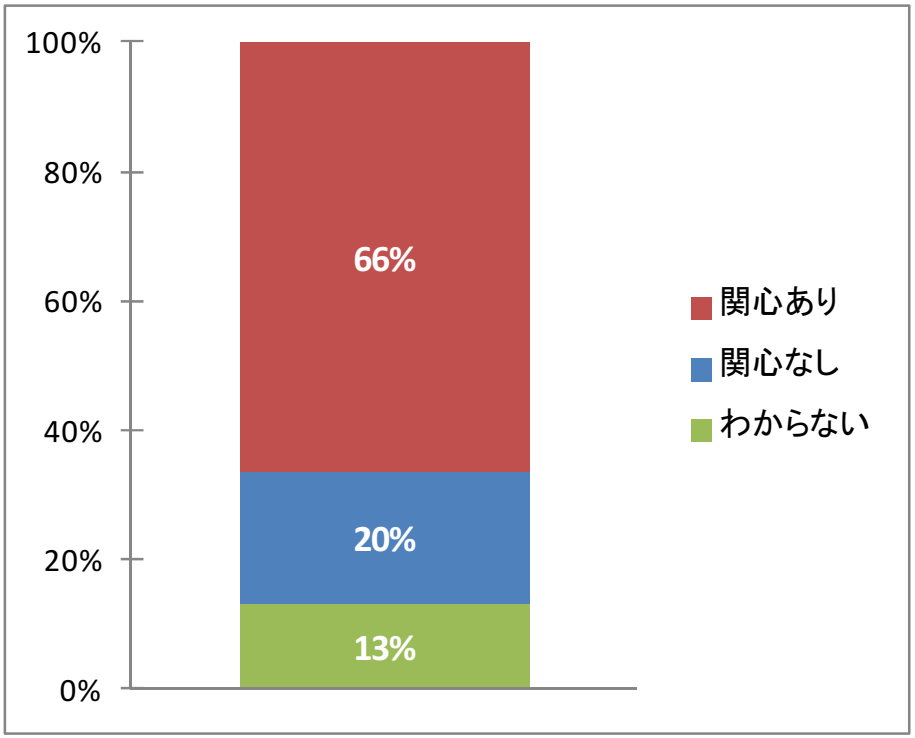
protiviti

COSO内部統制フレームワークの改訂

COSO内部統制のフレームワーク改訂（1）

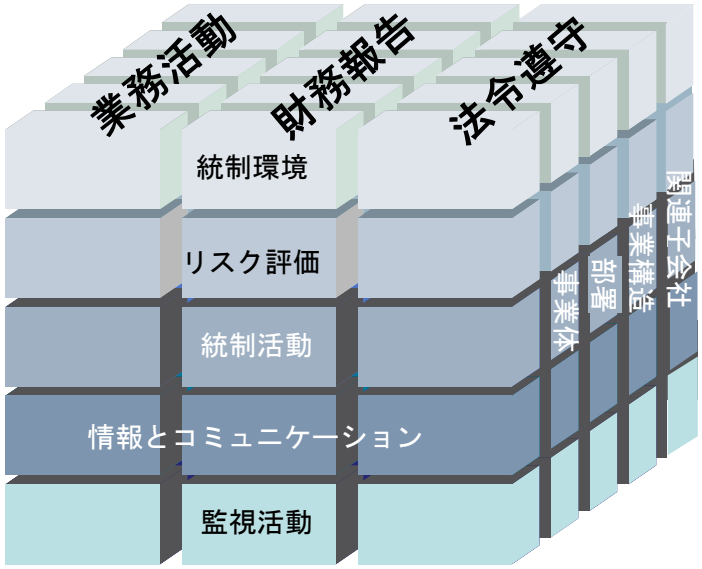
●COSO内部統制のフレームワーク改訂に関心はあるか

関心ありとする回答が66%



●COSO(トレッドウェイ委員会支援組織委員会)は内部統制フレームワーク改訂版を2013年5月にリリース。20年ぶりの改訂となる

●旧フレームワークは2014年より使用できなくなる



protiviti

COSO内部統制のフレームワーク改訂（2）

1992 内部統制－統合的枠組み
（COSO　内部統制フレームワーク）

2004 全社的リスクマネジメント－統合的枠組み
（COSO ERM）

2006 財務報告に係る内部統制
－中小規模公開ガイダンス

2009 内部統制システムモニタリングガイダンス
（2009.1）

2013 改訂版　内部統制－統合的枠組み
（COSO　内部統制フレームワーク）

COSOは、
- 内部統制、
- 全社的リスクマネジメント
- 不正防止

のフレームワークとガイドラインを策定する活動を実施

フレームワーク・ガイダンスの意義

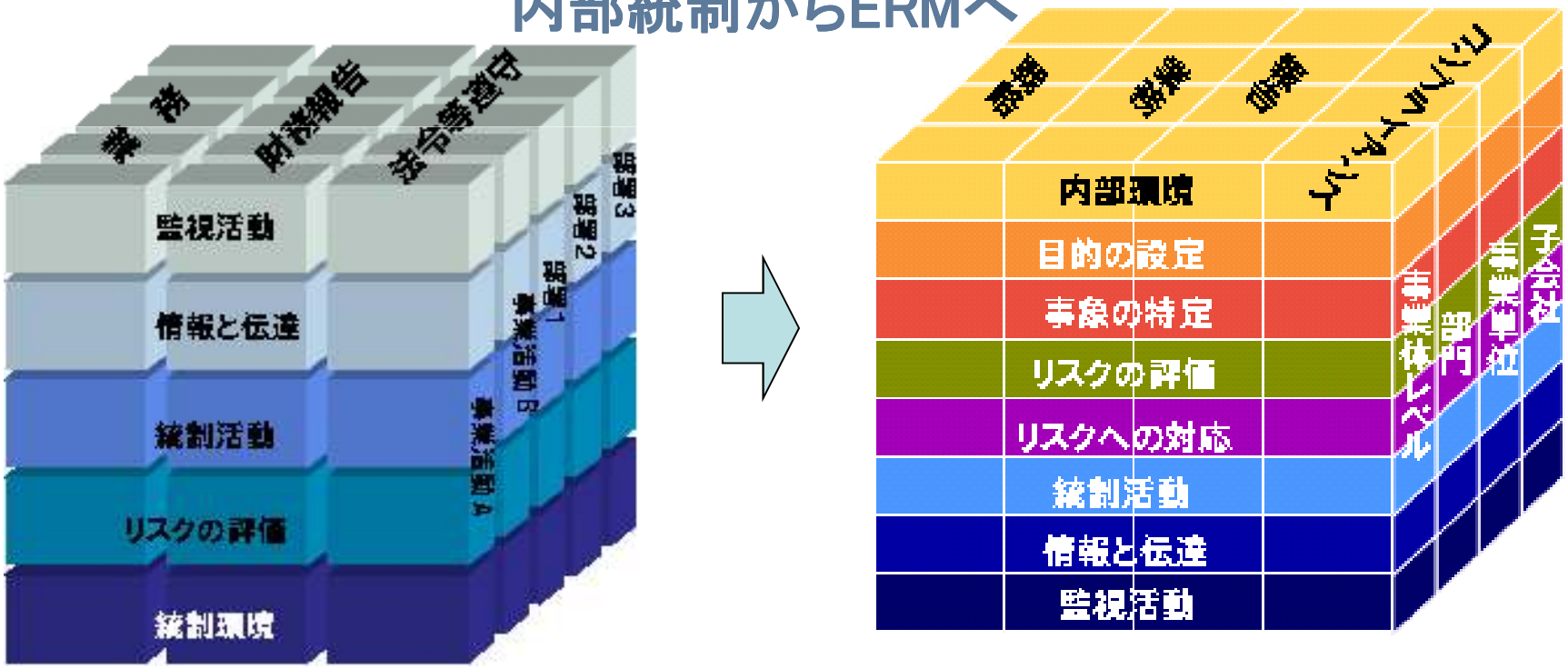
『共通の言語の提供』
『明確な方向性・指針を示す』

protiviti

COSO内部統制のフレームワーク改訂（3）

- ERMのフレームワーク （COSO　ERM　　：　2004年）
  - ERMは組織全体のリスクを対象として、経営に重要な影響を与えるリスクを組織全体で統合的に管理する。
  - 内部統制はERMに包含される概念であり、必要不可欠な一部

内部統制からERMへ



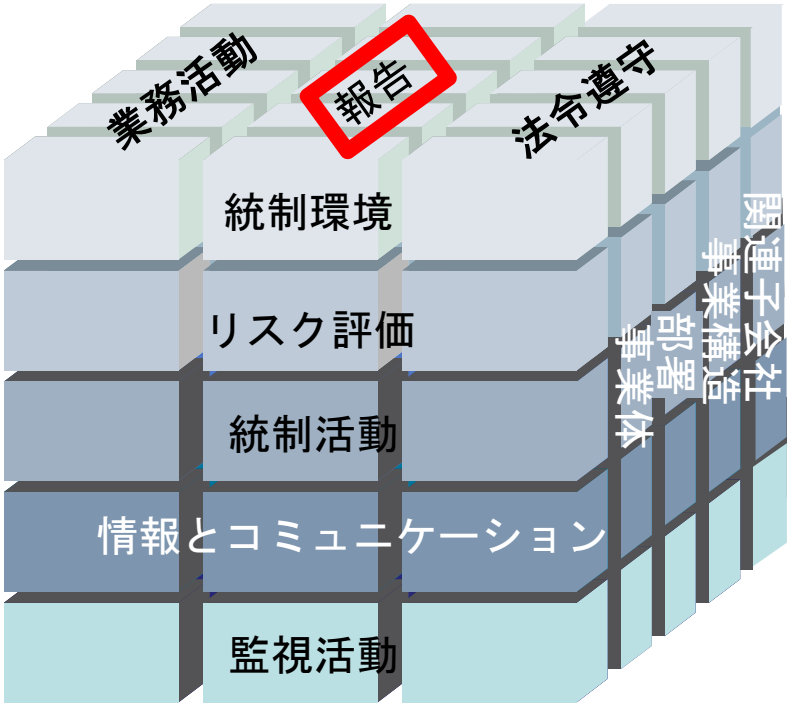
protiviti

COSO内部統制のフレームワーク改訂（4）

内部統制フレームワークの主な改訂ポイント

- 原則ベースのアプローチ～ **17原則と79の着眼点**
- **報告**の対象区分の拡大
- 内部統制の対象設定の**役割**の明確化
- **内部統制の有効性要件**を明示
- **ガバナンス**構造の強化
- 市場およびオペレーションの**国際化**の考察
- 異なる**ビジネスモデル**及び組織構造の考察
- **法律、規則、規制、基準**における要求と複雑性の考慮
- **能力と責任**への期待の考慮
- **テクノロジー**の関連性向上の反映
- **不正対応**への期待の認識強化
- **内部監査機能の強調**
- 外部財務報告（ICEFR）への適用事例の解説

COSO改訂版の内部統制の概念図



protiviti

COSO内部統制のフレームワーク改訂（5）

改訂版は有効な内部統制に不可欠な１７の原則を明示

統制環境	1. 組織は、誠実性と倫理観に対するコミットメントを表明する 2. 取締役会は、独立性を保持し内部統制の整備運用状況の監視を行う 3. 経営者は、組織構造、報告経路および適切な権限と責任を確立する 4. 組織は、有能な人材を惹きつけ、育成、維持にコミットする 5. 組織は、内部統制に対する責任を個々人に持たせる
リスク評価	6. 組織は、リスク評価のための適切な目的を明示する 7. 組織は、リスクの特定と分析を行う 8. 組織は、不正リスクを評価する 9. 組織は、リスクの重要な変化を特定し、分析する
統制活動	10. 組織は、リスクを許容可能水準まで低減する統制活動を選択整備する 11. 組織は、テクノロジに係る全般統制活動を選択し整備する 12. 組織は、期待を明記した方針及び手続のもとで統制活動を展開する
情報と伝達	13. 組織は、関連性のある質の高い情報を入手、作成して活用する 14. 組織は、内部統制の目的と責任分担を含む情報を組織内部に伝達する 15. 組織は、構成要素の機能に影響を与える事項を組織外部に伝達する
モニタリング活動	16. 組織は、構成要素が存在し機能していることを確かめるため継続的評価及び/又は、独立的評価を、選択、適用、実行する。 17. 組織は、適時に不備を評価し、是正措置の責任ある者に伝達する

protiviti

COSO内部統制のフレームワーク改訂（6）

改訂版は、原則の重要な特徴を明示
～着眼点（point of focus）

統制環境

1．組織は、誠実性と倫理観に対するコミットメントを表明する。

着眼点（*Points of Focus*）：
- トップの姿勢を示す
- 行動規範を確立する
- 行動規範の徹底状況を評価する
- 行動規範からの逸脱には適時に適応する

- この着眼点は、適合あるいは関連しないこともあり、その他の着眼点が特定されることがあるかもしれない。
- 着眼点は、内部統制の設計、導入、実施を容易にすることがあるかもしれない。
- **着眼点が考慮されていることを別途評価することを要請するものではない。**

COSO内部統制のフレームワーク改訂（7）

COSOのガバナンス、ERM、内部統制の関係

- ERMと内部統制の区別は維持し、両フレームワークは補足的関係
- 戦略設定、戦略目的およびリスク選好は、内部統制のフレームワークの範疇ではなく、ERMの範疇
  - リスク選好は、ビジョン・ミッション達成のために経営者が戦略目的策定する際の道標
  - リスク許容度は、戦略目的達成のために受け入れ可能なリスクレベル
- 改訂版内部統制フレームワークにおいては、戦略目的策定とリスク許容度は内部統制の一部分ではなく、有効な内部統制の前提であるとしている。

新COSOに示される位置づけ

COSO内部統制のフレームワーク改訂（8）

改訂版は、有効な内部統制の要件を明示

- 有効な内部統制の要件
  - **それぞれの構成要素と関連する原則が存在し、機能していること（ present and functioning ）**
  - **５つの構成要素が、統合された形で、共に運用されていること（ operating together, in an integrated manner)**
- それぞれの原則はすべての事業体に適合する前提。
- 構成要素が共に運用されているとは
  - すべての構成要素が存在し、機能している　さらに
  - すべての構成要素に関連する**不備（ deficiency ）**を累積したとしてもその結果が**重要な不備（ major deficiency ）**と判断されない
- 重要な不備とは、事業体の当該目的を達成する可能性がかなり低くなるような不備（一つまたは複数の内部統制の不備の組み合わせ）

ガバナンス・リスク・コンプライアンス（GRC）への取り組み

GRCへの取り組み（1）

GRCとは？

- **G（ガバナンス）、R（リスク）、C（コンプライアンス）**の略。米国リサーチ会社のガートナー社が最初に提唱したといわれる。
- GRCは、企業のコンプライアンス（法令順守）やガバナンス（企業統治）、リスク・マネジメントにかかわる業務**を一元的に管理するという概念**。
  - 取締役および執行役が総合的なリスクの視野を得られるように、別々の部門で行われてきたリスク管理機能を協働させ、分断・断片化されている取り組みを、連携・統合化させること
  - ERPベンダーや、GRC専業ベンダーが複数の法規制対応に必要な情報をまとめて管理するソフトのコンセプトとして展開している。
- 企業が目指しているのは

より強固・効率性の良い内部統制や企業価値への貢献を目的として、G（ガバナンス）、R（リスクとコントロール）、C（コンプライアンス）を包括的にとらえ、相互に連携を取りながら、重複なく効率的に進めていく一連の活動・仕組み・システム

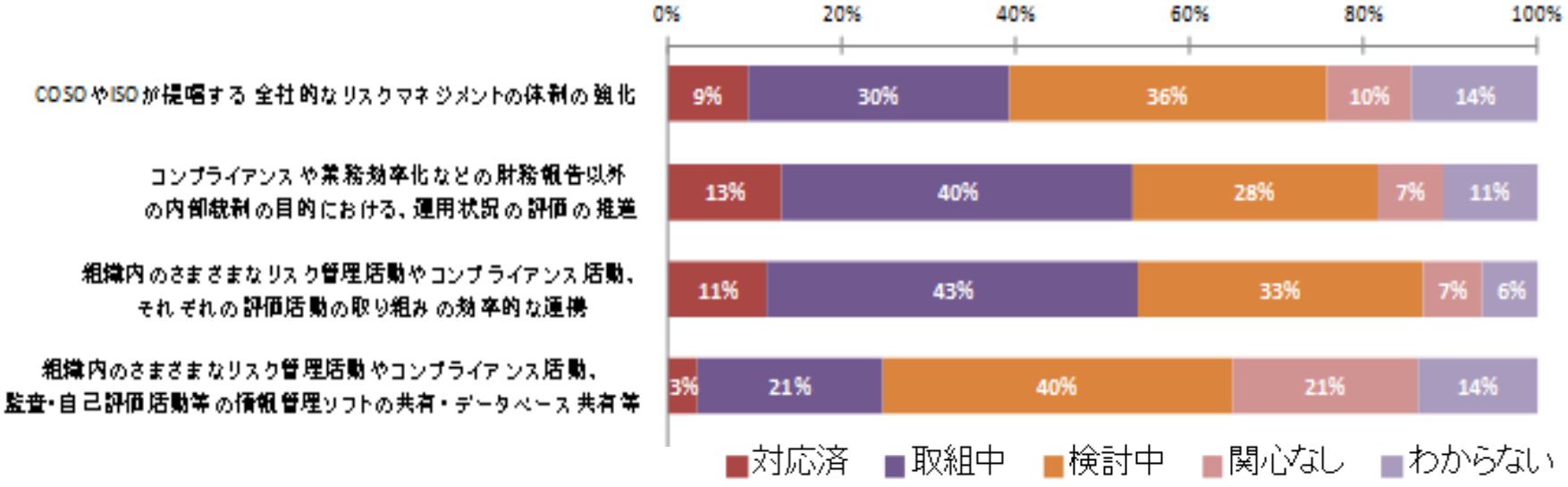
GRCへの取り組み（2）

- 対応済・取組中との回答が39%、検討中との回答を合わせ75%

  → 全社的リスクマネジメントの必要性が広く認識されている。

- 半数以上の回答企業が、財務報告以外の内部統制目的の運用状況評価を推進し、リスク管理やコンプライアンス活動の評価との連携に取り組んでいる。

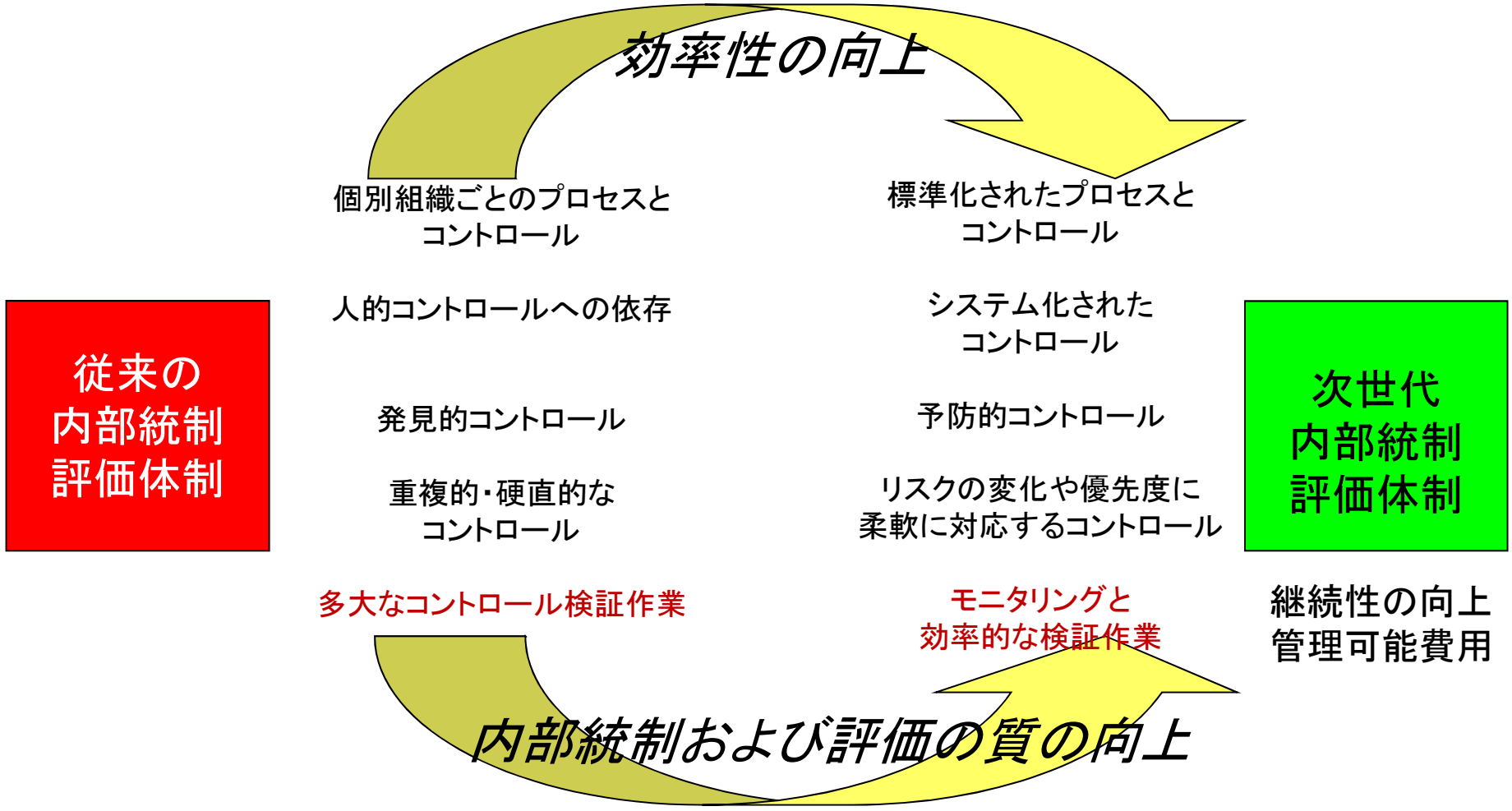
- それらの取り組みを共通のシステムやデータベースで実施しているところはまだ3%



protiviti

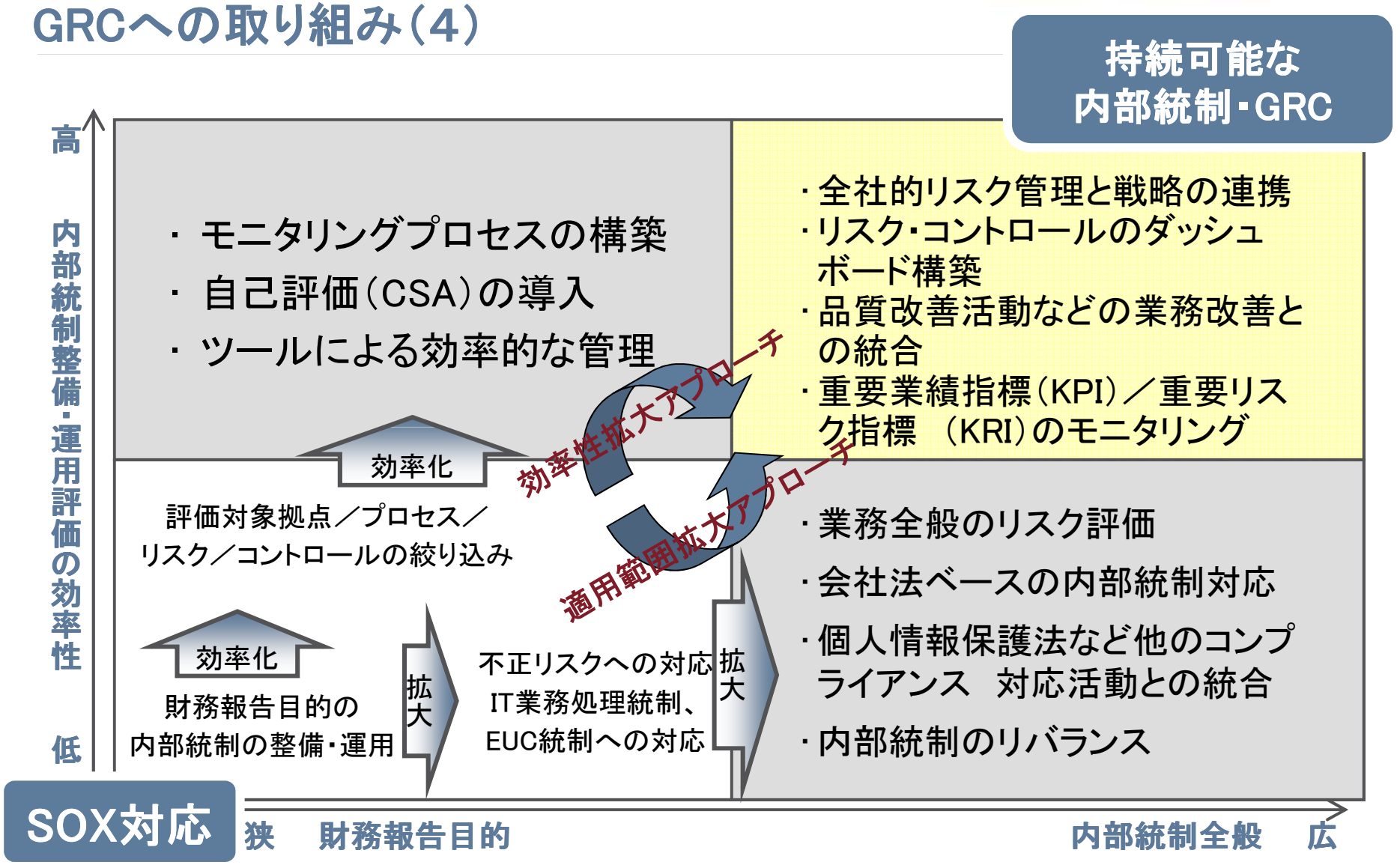
GRCへの取り組み（3）

内部統制評価の内製化と並行して、内部統制評価の効率化を多くの企業が進めている。



protiviti

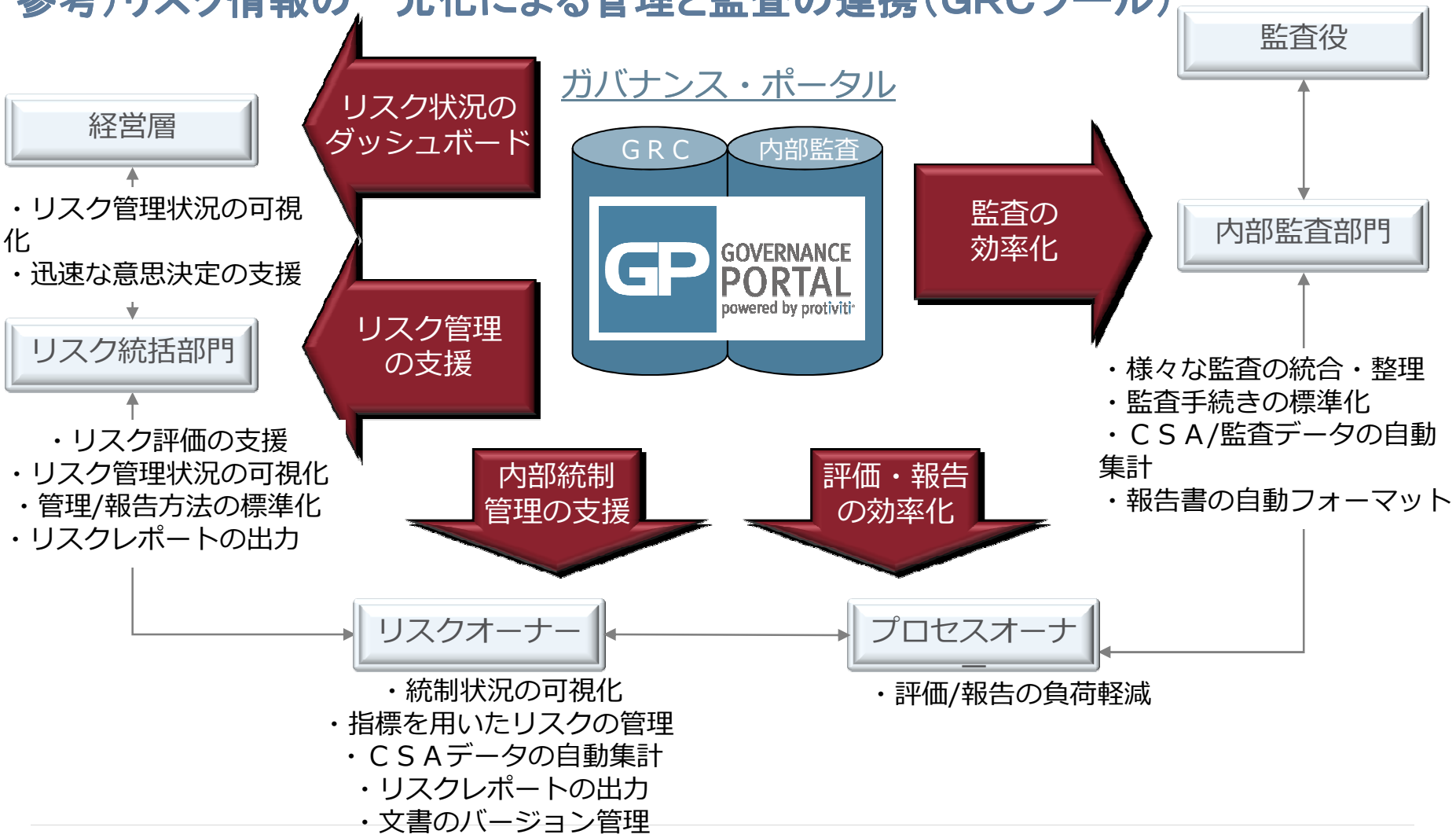
GRCへの取り組み（4）



protiviti

GRCへの取り組み（5）

参考）リスク情報の一元化による管理と監査の連携（GRCツール）



protiviti

おわりに

- SOX対応は、コンプライアンスの強化や、プロセス・業務の効率性・有効性を向上させる等、多くの効果をもたらしたことは確かである。
- 費用対効果でみると、必ずしも各企業が従来の取り組みに満足していないため、引き続き、それぞれの目的にかなった効率化の推進が課題。
- GRCへの取り組みについては、「対応済」とする回答は決して多いとは言えない状態であり、その取り組みはまだ発展途上。中長期経営計画との連動や企業価値向上のための統合的取組が不可欠である。
- SOX対応によって得られたノウハウ・知見を、内部統制全般の改善・経営効率向上に活かし、企業活動の向上に資するGRCへ展開することが、経営の透明性と効率性を高めることにつながる。

Powerful Insights.
Proven Delivery.®

protiviti®

Risk & Business Consulting.
Internal Audit.