Deloitte.

ガバナンス・リスク・コンプライアンス（GRC）ソフトウェア導入事例

アミューズメント ／ 食品 ／ クレジットカード ／ 資源開発 ／ 配送

トーマツ.

目次

事例①：アミューズメントB社（連結売上高：約400億ドル）

概要：自社のブランディングの継続的な維持・強化を目的として、全世界に展開する複数の異なる事業部門に対するコンプライアンスプログラムを統合した。

背景

1. 自社が対応すべきコンプライアンスプログラムの多様化、複雑化により、各事業部門への負担が増大しており、各部門での対応品質維持に苦慮していた
2. 自社のブランド維持のために、各事業部門の負担を軽減しつつ、グループ全体のコンプライアンス強化を行う必要があった。

目的

1. それまで独立して実施していた、SOX法対応（IT全般統制）とPCIDSS、
2. 自社保有ライセンス許諾に関するSafe Harbor管理のコンプライアンスプログラムを単一のフレームワークをもとに統合要求事項として整理し、共通アセスメントで複数の法令規制要求事項に対応できるようにする。
3. これにより各事業部の負担軽減と全社としてのコンプライアンスを強化

アプローチ

1. 各コンプライアンスプログラム（SOX、PCIDSS、SafeHarbor）の要求事項を単一のポリシーとして整理した（特にエビデンスの重複の面を重視した）
   ※　単なるポリシーの制定にとどまらず、それぞれの施策における各事業部へのアセスメント項目や収集するエビデンスの内容まで踏み込んだ
   ※　各施策での要求事項の重複を排除するだけでなく、施策横断的に抜け・漏れを確認し、それらに対する要求事項、アセスメント項目を追加した
2. 制定したポリシーをもとに各施策の推進部門と対象部署での業務フローを整理した。
3. 統合ポリシー、業務フローをGRCソフトウェアに実装し、施策運用の効率化を図り、その分各事業部との直接的なコミュニケーションを実施した。

成果

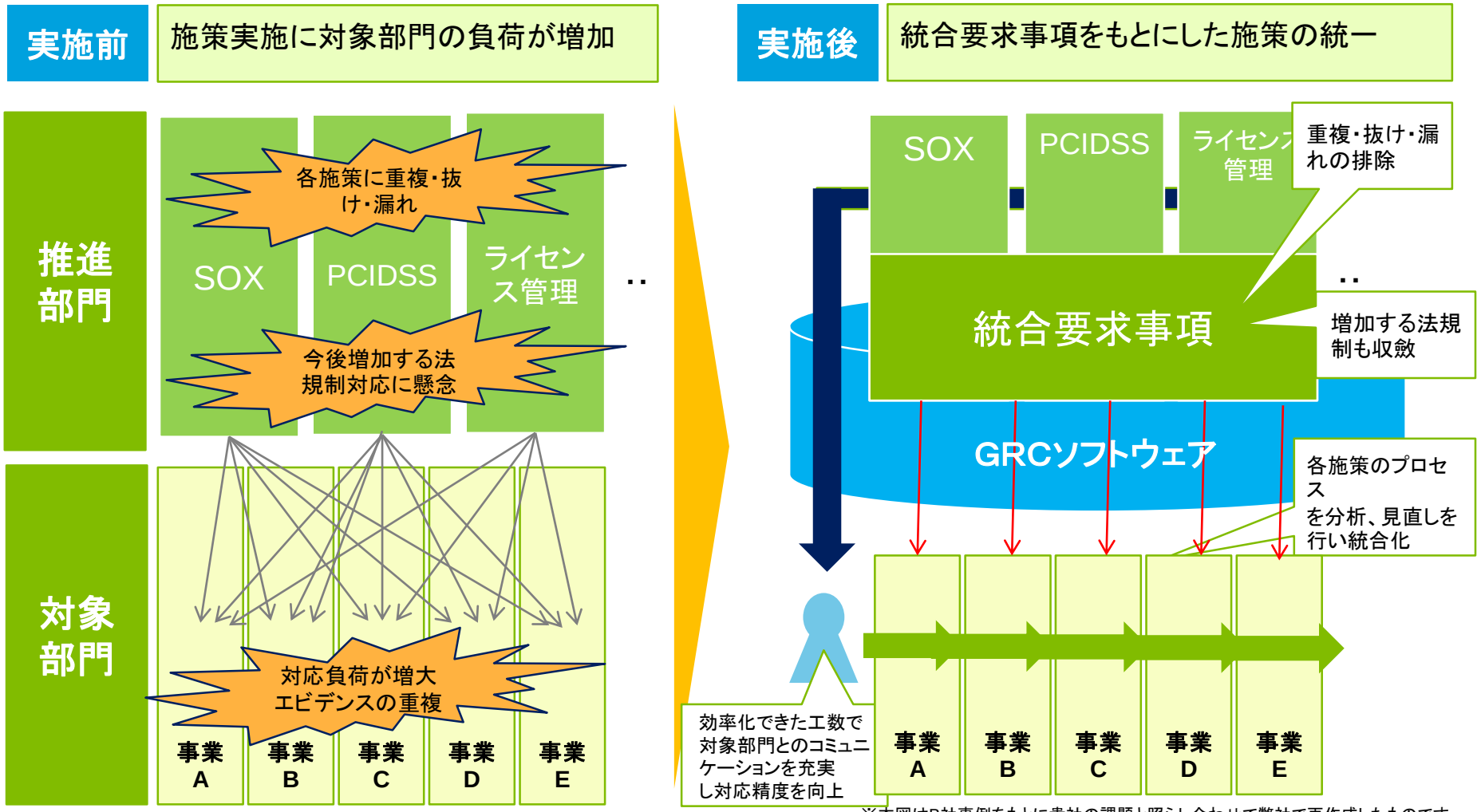
1. 効率化：評価活動・エビデンス収集の効率化による、各施策推進部門と対象部門の負荷軽減が実現できた
2. 対応の強化：GRCソフトウェア（Archer）への情報一元管理により発見事項（問題）の早期把握と解決の早期化を行った
3. 意識改革：効率化できたコンプライアンス担当者の時間をエンドユーザへのプログラム徹底とコミュニケーションの向上に活用することで、全社的な対応レベルの底上げを行った
   ※　さらに将来的に発生する対応すべき法令・規制対応にも同ポリシーに収斂させることで継続的な効率化と対応力向上が期待される

ポイント

情報管理：各施策で重複する要求事項、アセスメント項目を統合要求事項として再整理し、可能な範囲で統合を行う
情報伝達：統合要求事項をもとに現行の各施策の対象と業務フローを見直し、1回のアセスメントで複数の施策に対応できるようにする。
GRCソフトウェアを活用することで、推進部門と対象部門の業務効率化を図り、効率化できた時間を各部門とのコミュニケーションにあてた

事例①:アミューズメントB社　～効率化実施イメージ～

施策横断的な統合要求事項をもとに施策自体の統合を実現



※本図はB社事例をもとに貴社の課題と照らし合わせて弊社で再作成したものです。
必ずしもB社の具体的な管理体制や施策を反映したものではありません

事例②：食品C社（連結売上高：約540億ドル）

概要：M&Aや合弁企業、さらにグローバル化など事業展開が複雑化する同社が経営層、各事業、地域・国の責任者に対する寄与を目的として、リスクマネジメント等の施策を統合し、報告・意思決定の迅速化を図った。

背景

1. 組織体系の複雑化により、自社が対応すべきリスクやコンプライアンス要件が増加し、全体が見えにくい状況となっていた。
2. 各事業、地域、国の責任者（Cクラス）が自身の職責で取り組むべきリスク、コンプライアンス対応状況を担当者に確認していたが、情報収集・加工に時間がかかり必要なタイミングで情報が入手できなかった。

目的

1. 経営層及び各組織の責任者にとって有用な内容とスピードでの報告を実施を目的として、それまで別個に実施していたさまざまなリスクマネジメント、コンプライアンス、ITセキュリティに関する施策を統合した。
2. 経営上の意思決定に役立つ報告をタイムリーに実施することで、上層部にリスク、コンプライアンス対応の重要性を意識づけた。

アプローチ

1. 中期計画等の戦略や経営層、各組織の責任者から発信されたメッセージをもとにトップマネジメントが意識すべきリスク、コンプライアンスの内容と、それを経営上の意思決定に役立てるために必要な情報について、その内容と速さについて分析し、各マネジメントに同意を得た。
2. 上記の内容と迅速性を確保するため、可能な限り施策の統合を行った。
3. 経営層、各組織の責任者への迅速・正確な報告を行う手段の1つとして、GRCソフトウェアを活用した。

成果

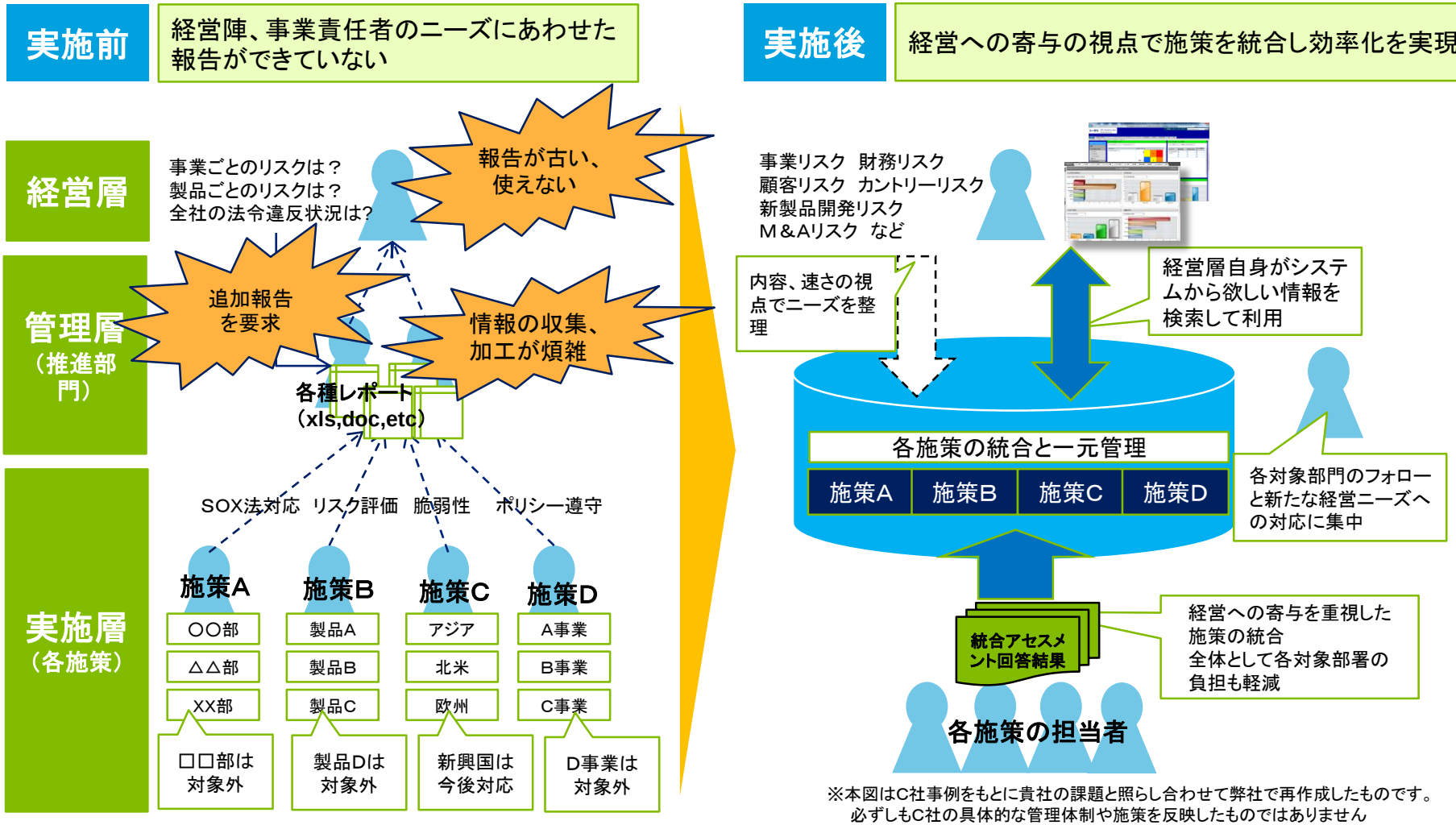
1. 20以上のリスクアセスメントプロセスを統合
2. 初年度で50%の対応コスト削減
3. 10以上の複雑な組織構造に対して統合管理を実現
4. 20以上の組織、40以上の事業部門に対してリアルタイムなレポート配信
5. 経営層へのリスク・コンプライアンス報告の迅速化

貴社の検討で参考にしていただきたいポイント

情報活用：経営に寄与する視点から情報の活用を促進する → Cクラスのニーズの把握とそれを実現するための報告の実現
情報管理：報告作成のための負荷の軽減→収集・加工に関する工数の削減

事例②：食品C社　～効率化実施イメージ～

経営に寄与する報告を実現するための情報活用の実現



※本図はC社事例をもとに貴社の課題と照らし合わせて弊社で再作成したものです。
必ずしもC社の具体的な管理体制や施策を反映したものではありません

事例③：クレジットカード事業G社（連結売上高：約300億ドル）

概要：グローバル展開している企業がGRCソフトウェアを導入し事業拠点ごとのコンプライアンス対応業務を統合・整理することで、コンプライアンス管理業務を強化・効率化した。

背景

1. コンプライアンス対応業務が複雑化・多様化する中で、グローバル展開している複数の事業拠点がそれぞれ別々にコンプライアンス管理業務を行っていたため、全社レベルの観点からコンプライアンス管理が行えず、重複する業務などもあり非効率であった。
2. リスク情報やコンプライアンス情報を管理するシステムも各事業拠点で別々であったため、リスク情報やコンプライアンス情報を全社レベルで包括的に把握することが困難であった。

目的

1. 事業拠点ごとにそれぞれ行われているコンプライアンス対応業務を統合し、コンプライアンス管理業務の効率化を図る。
2. 事業拠点ごとに別々のシステムに入力していたリスク情報やコンプライアンス情報を一元管理し、全社レベルで包括的に把握できるようにする。

アプローチ

1. 事業拠点ごとに行われて重複しているコンプライアンス対応業務を統合するために、GRCソフトウェアを導入するとともに、システムへの入力者やプロセスオーナー等の業務プロセスを全社レベルでの観点から整理し、事業拠点間や部門間の役割を明確にした。
2. リスク情報やコンプライアンス情報を全社レベルで包括的に把握するために、PCI DSS（クレジット業界におけるグローバルセキュリティ基準）やSOX等のコンプライアンス情報を全事業拠点共通のGRCソフトウェアに一元管理し、入力されたリスク情報やコンプライアンス情報を紐付けて、事業拠点ごとの比較や、事業拠点にまたがって共通に認識されるリスクを見える化した。

成果

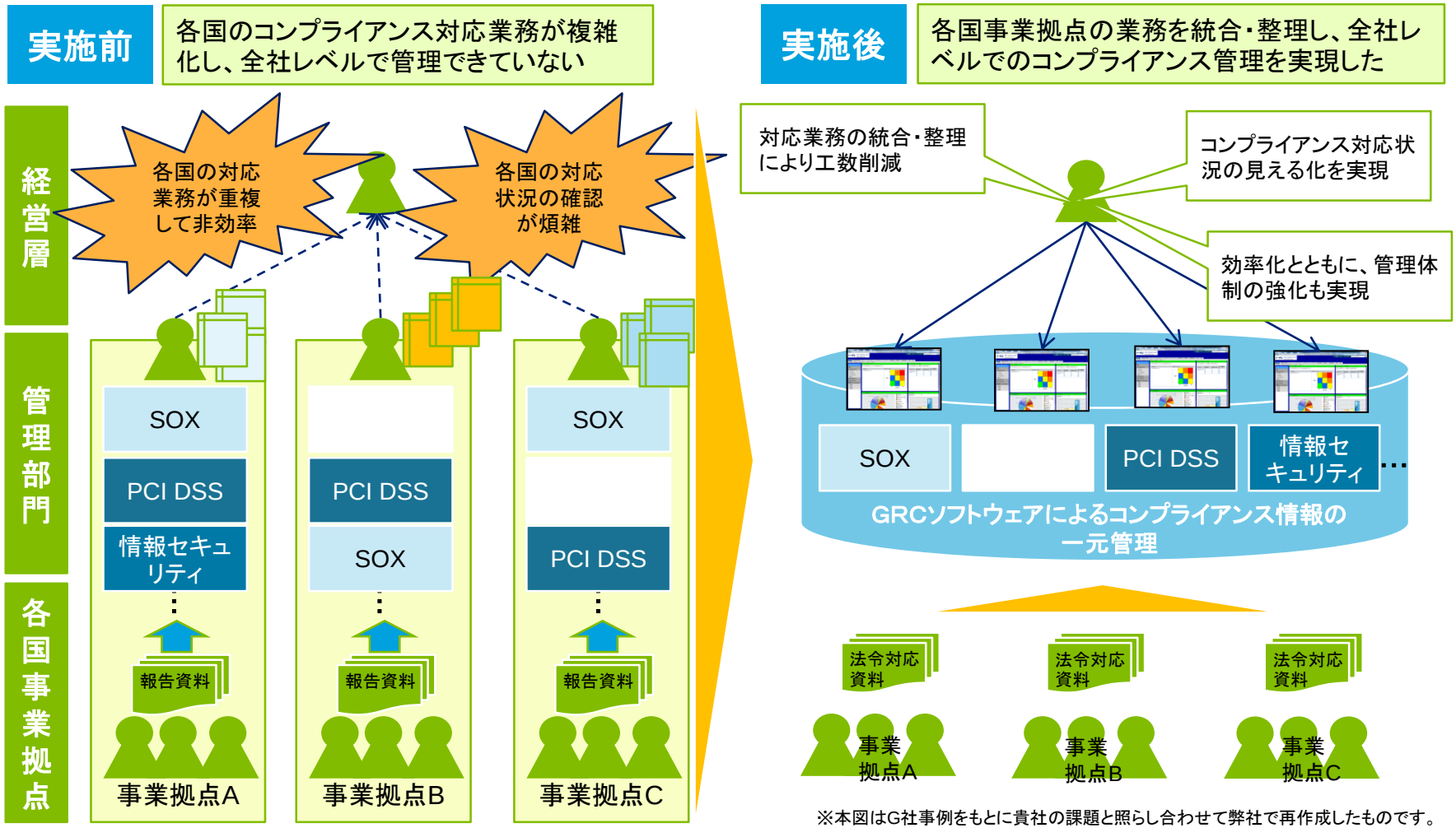
1. 全社レベルでの観点から業務プロセスを整理し、事業拠点間や部門間の役割を明確にしたため、業務の重複が統合され、コンプライアンス管理業務が効率化した。
2. リスク情報やコンプライアンス情報が全社共通のGRCソフトウェアで一元管理されたため、データの紐付けが容易となり、リスク情報やコンプライアンス情報を全社レベルで包括的に把握することができるようになった。

貴社の検討で参考にしていただきたいポイント

情報管理：GRCソフトウェアを導入することで情報を一元管理することができ、リスク情報やコンプライアンス情報の紐付けが容易となる。
情報伝達：全社共通のシステムに情報が集約されるため、リスク管理やコンプライアンス管理の状況を全社レベルで包括的に把握できる。

事例③:クレジットカード事業G社　～統合・整理イメージ～

各国の事業拠点のコンプライアンス対応業務を統合・整理



※本図はG社事例をもとに貴社の課題と照らし合わせて弊社で再作成したものです。
必ずしもG社の具体的な管理体制や施策を反映したものではありません

事例④：資源開発H社（連結売上高：約280億ドル）

概要：SOX対応を手作業で行っていた企業が、GRCソフトウェアを導入してSOX対応の強化・効率化を実現した。

背景

1. SOX対応における事業拠点の選定や重要な勘定科目の特定等の業務がすべて手作業で行われていた。
2. 各拠点の業務プロセスの定義にばらつきがあり、評価結果の拠点間比較が困難であった。
3. 四半期単位での内部統制自己評価結果等のレポートをリアルタイムに閲覧することができず、ビジネス環境の変化に対応するための経営の迅速な意思決定に役立たなかった。

目的

1. GRCソフトウェアを導入することで、SOX対応に必要なデータを自動化させ、SOX対応の効率化を図る。
2. 業務プロセスの定義の共通化を図り、SOX対応を見える化する。
3. SOX対応の強化・効率化により、SOX対応に関連するレポートをリアルタイムに提供して経営の迅速な意思決定に役立てる。

アプローチ

1. 各事業拠点で共通のGRCソフトウェアを使用して、今まで様々な形式で作成されていたSOXの文書を均一化し、各事業拠点の財務情報を紐付けることでSOX対応に必要なデータを自動化し、事業拠点の選定や重要な勘定科目を特定する業務を効率化させた。
2. SOX対応の過程を見える化するために、業務プロセス及びサブプロセスの定義を共通化し、同一事業については複数の拠点にまたがっても同じ視点で見られるように業務フローを整理した。
3. リアルタイムでのレポート閲覧を可能とするために、評価活動は複数の事業拠点で同一時期に実施する等、方針や規律を作り徹底した。

成果

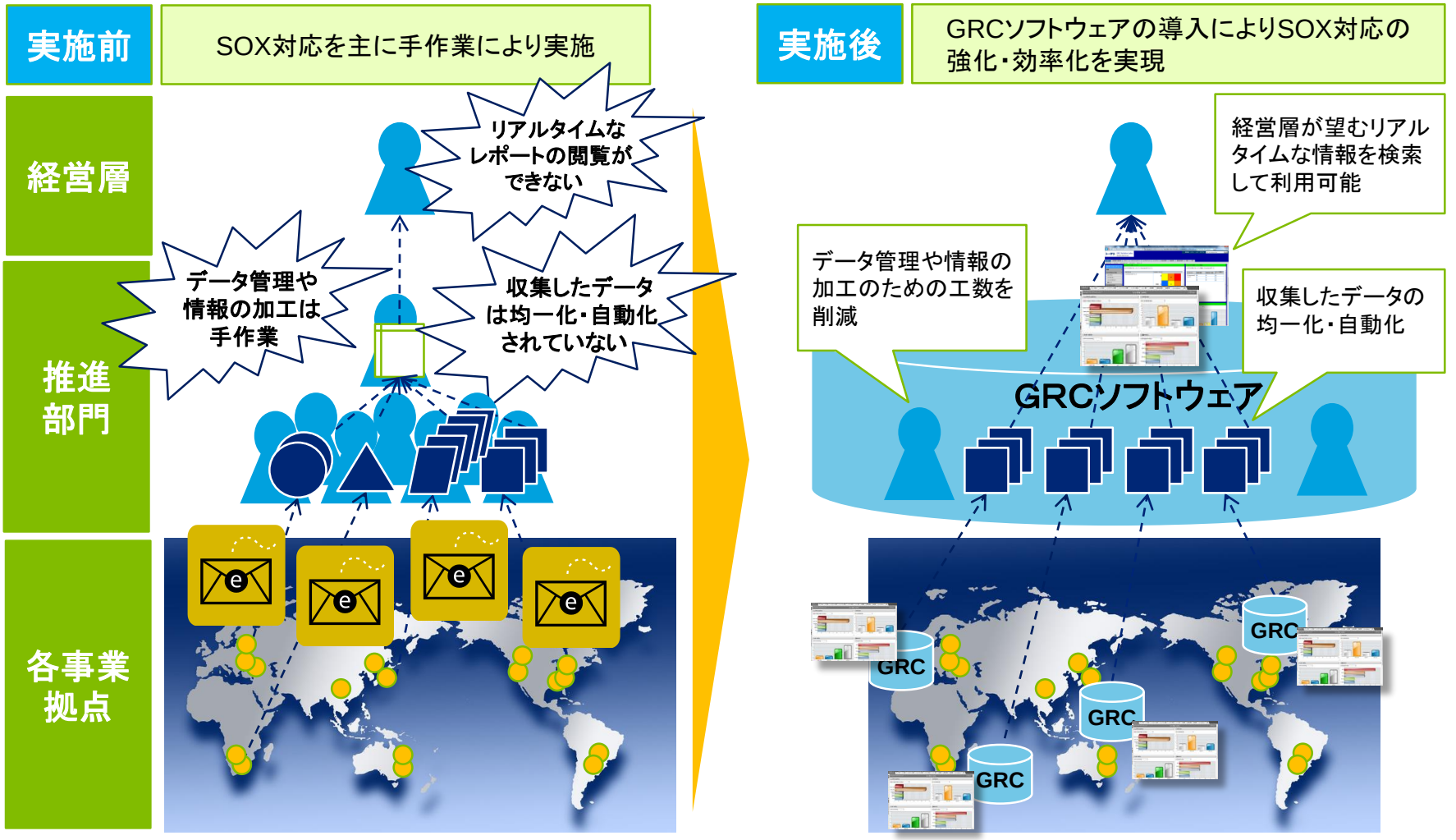
1. 各拠点から収集するデータの均一化・紐付けにより、SOX対応が効率化された。
2. SOX対応が見える化されたことにより、内部統制の有効性や信頼性が向上した。
3. SOX対応における方針や規律の徹底により、SOX対応に関連する情報をリアルタイムに取得できるようになった。
   例1）SOX対応の現場で必要な情報がリアルタイムで取得できるため、推進部門に不備等の重要情報がタイムリーに伝達されるようになった。
   例2）経営層が望むレポートをリアルタイムに閲覧できるため、経営の迅速な意思決定に役立てることができた。

貴社の検討で参考にしていただきたいポイント

情報管理：GRCソフトウェアを導入することにより、グローバル展開している各拠点から収集したデータが均一化され、レポート作成のためのデータ管理・加工に関する工数を削減することができる。
情報伝達： SOX対応が見える化されることにより、地理的に離れた対象部署、子会社等の実態の把握が可能となる。
情報活用：作成されるレポートはリアルタイムに提供され、分析を行うことでリスクを未然に防ぐことが可能となる。

事例④：資源開発H社　～SOX対応の強化・効率化実施イメージ～

SOX対応を強化・効率化するための情報管理の実現



※本図はH社事例をもとに貴社の課題と照らし合わせて弊社で再作成したものです。 必ずしもH社の具体的な管理体制や施策を反映したものではありません。

事例⑤：配送事業I社（連結売上高：約700億ドル）

概要：電子配送のビジネス戦略を強化している企業が、GRCソフトウェアを導入して外部委託先管理の強化を図り、ITリスクを事前把握して予防措置を行うことで情報セキュリティ関連のインシデントが減少した。

背景

1. 情報セキュリティマネジメントが徹底されていなかったため、情報漏えい等のITリスクが事前に把握できず、顕在化してから対処していた。
2. 電子配送は外部委託先への依存度が高いが、外部委託先管理スキルが低かったため、ITリスクを十分に把握できず、ステークホルダーに対してITリスクへの対応状況を説明することができていなかった。

目的

1. ITリスクが顕在化してから事後対応を行うのではなく、ITリスクを事前に把握し予防措置を講じる。
2. ITシステムの構築における外部委託先管理を徹底し、ITリスクの状態を包括的に認識してステークホルダーへの説明責任を果たす。

アプローチ

1. 網羅的かつタイムリーにITリスクを把握するために、情報セキュリティマネジメントのPDCAサイクルをシステムライフサイクルプロセスに組み込んだ。
2. ITリスクへの対応状況を包括的に認識するために、GRCソフトウェアを導入して、外部委託先の企業情報、外部委託先との契約情報、インシデント情報等を一元管理した。
   - 一元管理された様々な情報をITリスクに対応するための優先度の決定に利用した。
   - 把握したITリスクへの対応状況や予防措置をITリスクと紐付けて継続的なモニタリングを行った。

成果

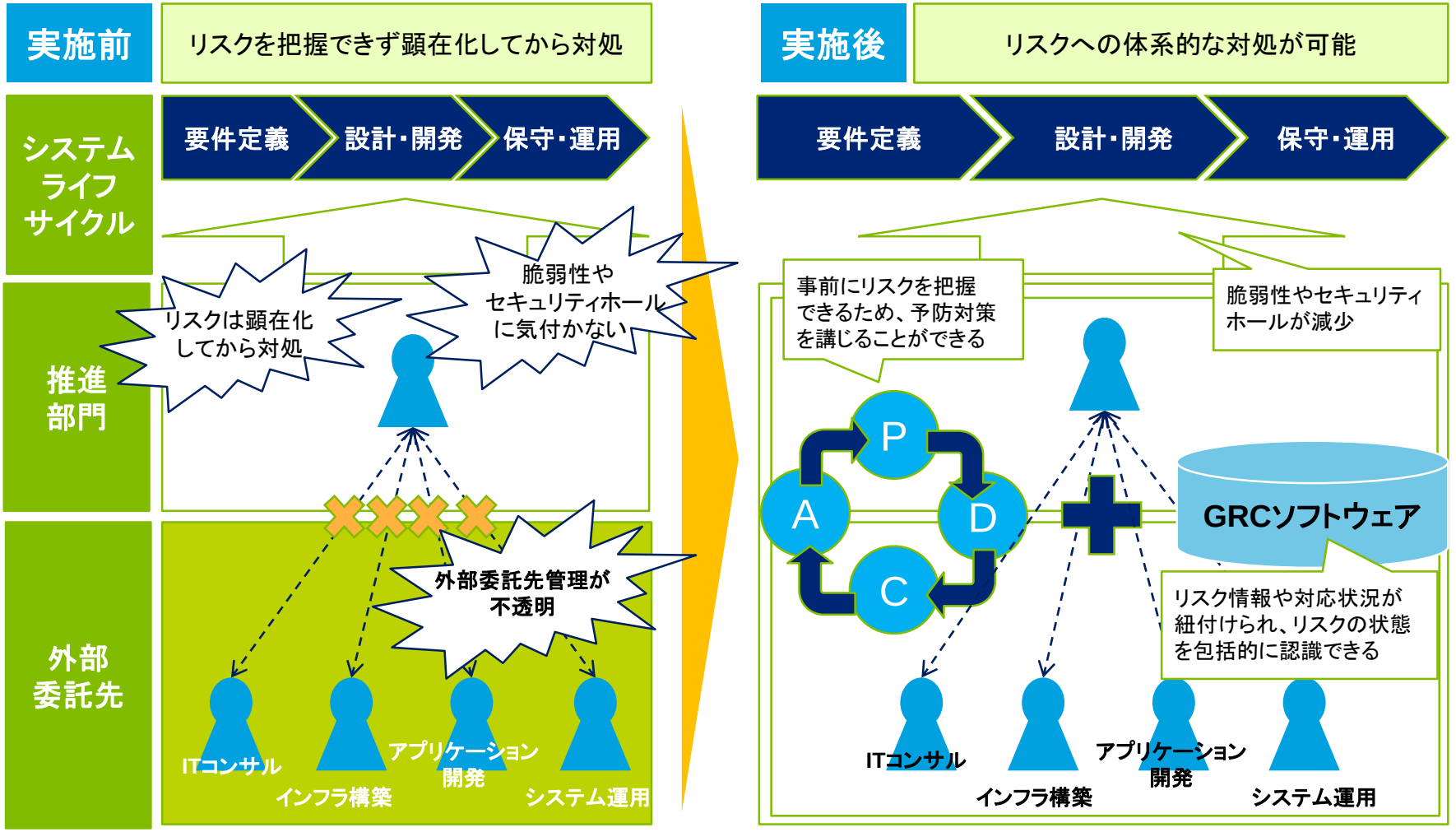
1. 情報セキュリティマネジメントを徹底して事前にITリスクを把握することで予防措置を講じることができ、情報セキュリティ関連のインシデントが減少した。
   - 構築したITシステムの脆弱性やセキュリティホールが減少した。
   - 外部委託先への依存度が高いシステムの品質を一定レベルに担保することができるようになった。
2. 外部委託先管理を強化したことにより、ITリスクをどう把握しどう対処しているかをステークホルダーに説明できるようになった。

貴社の検討で参考にしていただきたいポイント

情報管理：GRCソフトウェアの導入により、外部委託先の企業情報、外部委託先との契約情報、インシデント情報等の関連付けが容易となり、把握したITリスクの優先順位の決定や対応状況の継続的なモニタリングに役立つ。
情報伝達：情報セキュリティマネジメントのPDCAサイクルと組み合わせることにより、外部委託先との関係に伴うリスクやその対応状況を見える化できる。

事例⑤:配送事業I社　～外部委託先管理の実施イメージ～

GRCソフトウェアを利用した外部委託先管理の実現



※本図はI社事例をもとに貴社の課題と照らし合わせて弊社で再作成したものです。 必ずしもI社の具体的な管理体制や施策を反映したものではありません。

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、税理士法人トーマツおよびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約8,500名の専門家（公認会計士、税理士、弁護士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約220,000名を超える人材は、“making an impact that matters”を自らの使命としています。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細は www.deloitte.com/jp/about をご覧ください。

有限責任監査法人トーマツ 東京事務所エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントの国際規格であるISO/IEC27001の認証を取得しました。
2009年4月1日には、デロイト トーマツ リスク サービス株式会社をこの認証範囲に含めております。

IS 501214 / ISO (JIS Q) 27001

有限責任監査法人トーマツ 東京事務所におけるBCP/BCMサービス提供部門およびデロイト トーマツ リスクサービス株式会社は、2011年3月11日に事業継続マネジメントシステムの規格であるBS25999-2:2007の認証を取得し、2013年2月19日に国際規格であるISO22301:2012の認証を取得しました。

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited