GRCツール／システムの導入で内部監査は高度化できるのか

――既存ツール／システムを活用して内部監査のDXを推進

PwCあらた有限責任監査法人
ガバナンス・内部監査サービス部
ディレクター　**岩永 摩美**

はじめに

急激な在宅勤務の浸透、リモート監査の適用対象の拡大を受け、「GRCツール／システム」の導入を検討する企業が増えてきており、問い合わせも数多くいただいています。たしかにGRCツール／システムを使えば内部監査のDXを高度化できますが、闇雲に導入すればよいというものではなく、自社の成熟度に応じてどのように導入すべきか検討する必要があります。本稿では、具体的な事例を交えて内部監査のDX推進のステップについて解説します。

なお、文中の意見に係る部分は筆者の私見であり、PwCあらた有限責任監査法人および所属部門の正式見解ではないこと、あらかじめご理解いただきたくお願いします。

1 ステップ1：GRCツール／システムとは何なのか

筆者は、俗に「GRC領域」と呼ばれる分野で長年アドバイザリーサービスをご提供したり、事業会社で内部監査室長等を担当してきましたが、いまだにGRCツール／システムとは何ができるツール／システムであるのかを端的に言うことができません。皆さんは、GRCツール／システムという言葉はどういう意味で、何ができるツールだとお考えでしょうか？

そもそもGRC（Governance、Risk Management、Compliance）とは、企業における内部管理態勢を包括的に捉える概念です（**図表1**）。全社的リスク管理態勢の高度化、すなわち、企業の戦略目的の達成能力強化を図るためのフレームワークを指します。

従来の伝統的な企業もしくは企業グループにおいては、それぞれの担当機能部門が機能別に管理を行ってきました。しかし近年は、機能別管理の業務負担が増し、リスク管理も複雑化する傾向にあります。このため、全社で一元的にリスク管理・コンプライアンス管理・内部統制を行う統合管理が求められています（**図表2**）。これが、eGRC（enterprise Governance Risk Compliance）システムツールが進化してきた背景としてあります。この文脈では、GRCツール／システムとは、GRCの各領域の管理をサポートするツールの総称ということになります。対象とする分野も幅広く、多彩なモジュール（機能）を含むため、ベンダーによってGRCツール／システムに含まれると認識しているモジュールは異なります。

図表3に、一般にGRCツール／システムに含まれることが多いモジュールの種類と利用目的をまとめました。このモジュール（機能）群を組み合わせて「ソリューション（アプリケーションパッケージ）」として販売されているものが「GRCツール／システム」ということになります。

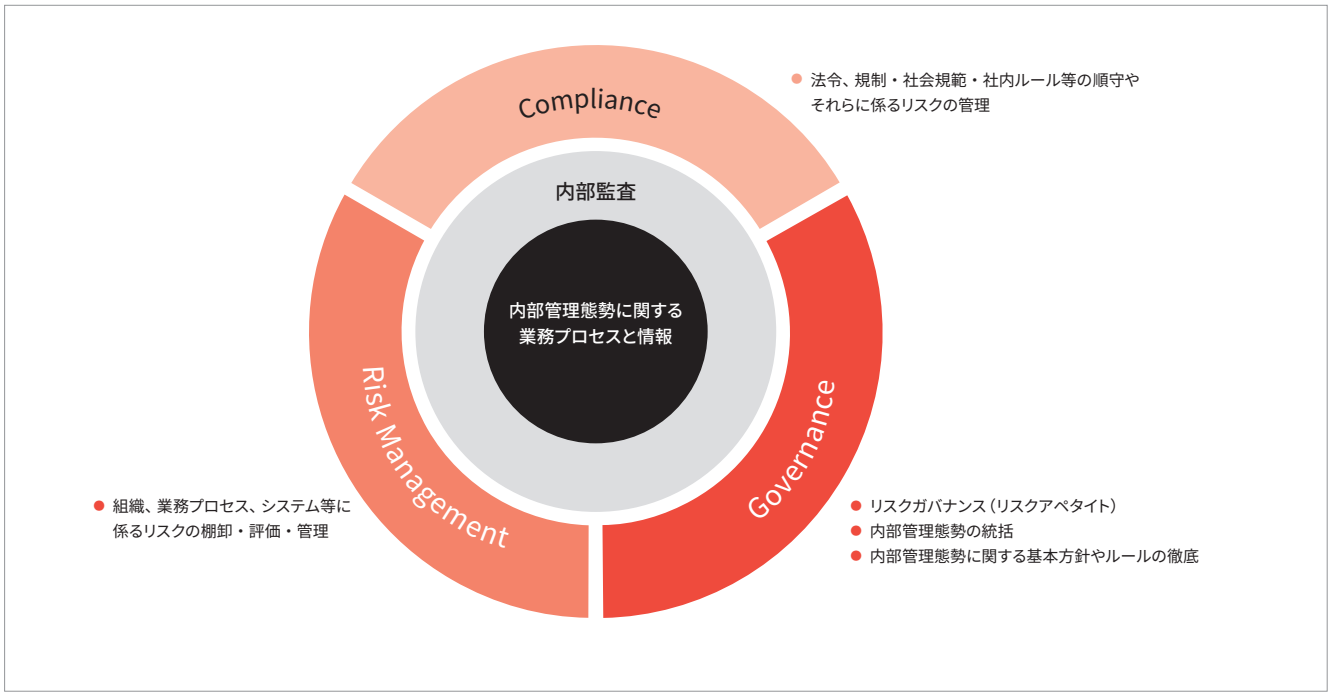
ここで注意が必要なのは、ベンダーによってGRCツール／

システムという言葉が指し示す機能が異なる点です。各種メディア記事や論文などを参照してみても、それぞれの筆者の立場によって意味するものは異なっています。また、同じ組織内で同じ名称を用いていても、違うものを指していることはよくあります。GRCツール／システムについて論じる場合は、その意味するものが具体的に何であるのか互いに確認する必要があります。

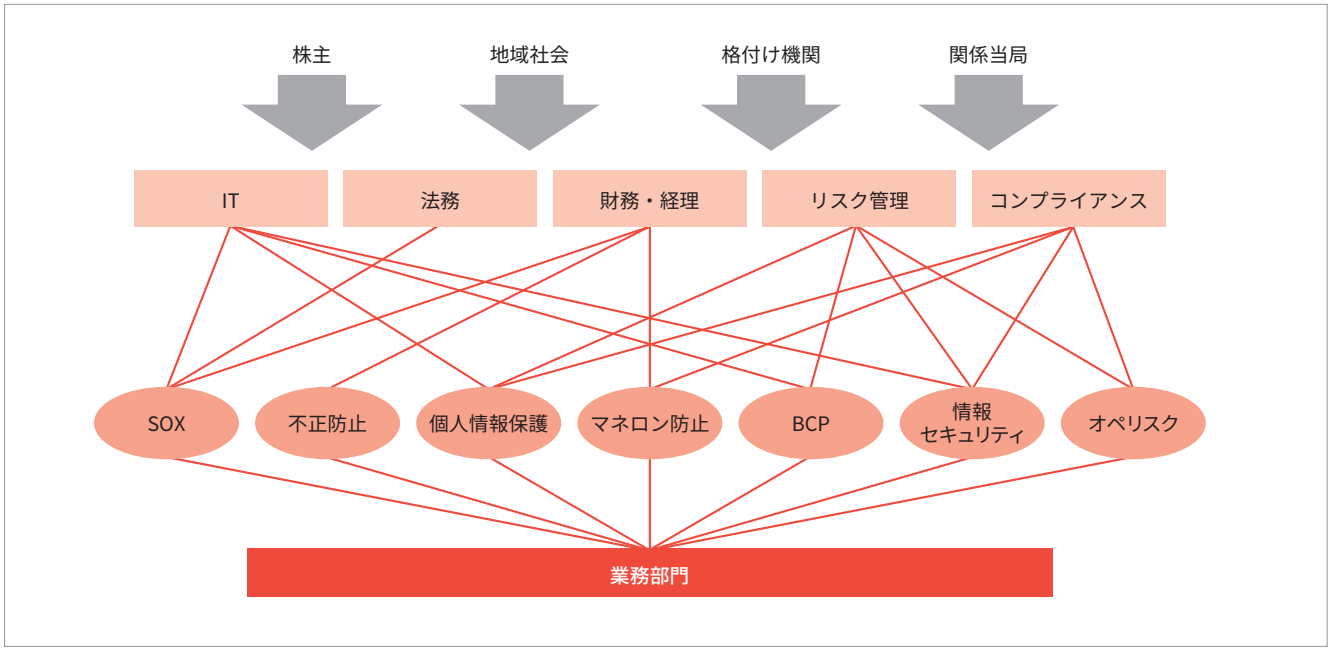
2 ステップ2：GRCツール／システムの導入による期待効果とは？

多くの組織では、GRC領域の活動を支援することができる情報システムがすでに社内に存在しています。では、これらのツール／システムと、GRCツール／システムと総称されるシステムとは何が違うのでしょうか。

図表1：GRCの全体概念



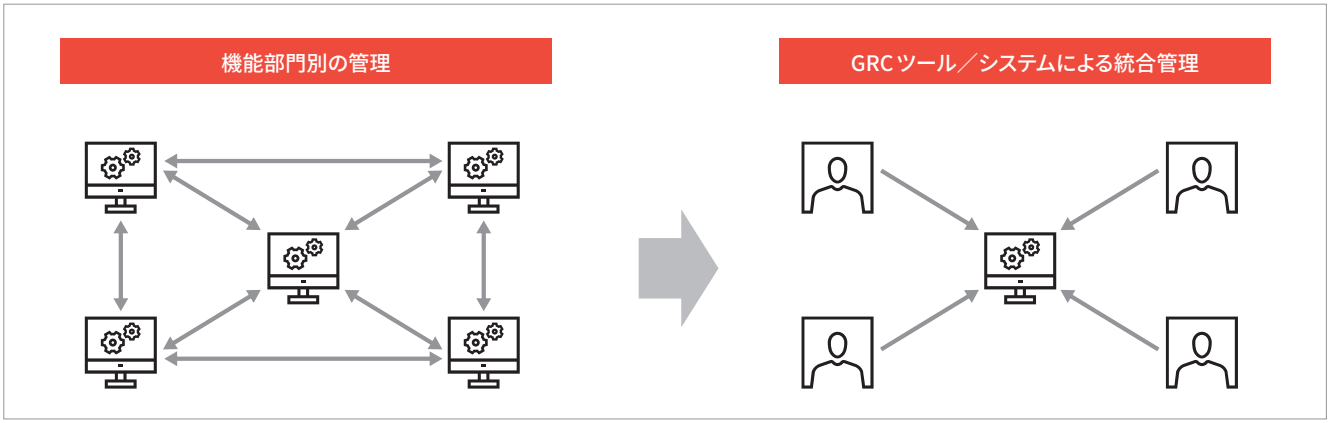
図表2：企業の業務部門における機能の統合



図表3：GRCツール／システムに含まれるモジュールの種類と利用目的

種類	利用目的
ポリシー管理	● 企業内のポリシーを集中管理 ● 法令、ガイドライン、社内規定、各種業務手順を体系化 ● 法令と社内ルール、ポリシー改訂等の自動化
コンプライアンス管理	● コントロールフレームワーク、管理手順やテスト計画を管理 ● 検出事項の識別、改善計画の管理
リスク管理	企業が認識するリスクに対して、リスクアセスメントの実施、リスク対応計画の策定、リスク対応の進捗状況や有効性評価などの一連の流れを管理
インシデント管理	日常的に発生した障害や、サイバー攻撃の記録を取得し、発生したインシデントの分析や改善事項を管理（インシデントの特定、インシデントの評価、調査状況の管理、インシデントの解決、インシデント傾向のレポートなど）
ビジネス継続管理	● 非常事態発生時に、必要な事業継続や災害復旧計画を指示し、迅速な対応をサポート ● 事業継続計画・災害復旧計画の文書化、計画の有効性の測定等、BCP活動を支援（事業影響度分析、事業継続計画の文書化、災害復旧計画の文書化、計画の有効性を検証、危機となるイベントを追跡、計画のメンテナンスを自動化）
委託先管理	委託先企業のデータを集中的に管理し、委託先企業のリスク評価や規程類、法令、ガイドラインへの準拠状況と関連性を明確化
内部監査管理	監査計画の策定から監査手続の実施、監査結果の報告プロセスについて、リソース管理、監査手続書の作成サポート、報告書のテンプレート等を管理
ITオペレーショナルリスク管理	● セキュリティ監視機器から送られるアラートの集中管理とインシデント対応のワークフローの自動化により、インシデント処理に必要な情報の共有、担当者間のプロセスフローの管理、インシデント対応状況のモニタリングや稼働管理等を実施 ● 既存の脅威情報の分析、管理を行い、企業に対する攻撃や不安要素を早期に検知
その他管理機能	● コンプライアンス意識調査 ● 従業員満足度調査 ● 内部通報受付システム ● グループ会社の企業情報管理 ● IT資産管理 ● IoTデバイス管理 ● 情報セキュリティパッチ管理 ● 法令一覧管理 ● 上記の各データのビジュアライズ機能

図表4：機能部門別の管理とGRCツール／システムによる一元的な統合管理



GRCツール／システムを導入すれば、機能部門別のリスク管理・コンプライアンス管理・内部統制を一元的に統合管理できるようになります（**図表4**）。さらに、以下の5つのメリットも享受できるようになると考えられています。それぞれの期待される効果の例も挙げておきます。

- **情報の一元化：**共通GRCプラットフォームに情報（リスク、内部統制、各種規程類、検出事項等）を集約し、ユーザーが容易に取得・利用可能にする
- **業務の標準化と効率化：**全社共通のテンプレート（統一されたバージョン）を使用し、共通の業務プロセスで運用が可能になる
- **業務の自動化：**リスクに基づく範囲設定、データ収集、アセスメントのスコアリング、アセスメントによる発見事項の記録等を自動で通知する。また、承認のワークフローを自動化し、機能部門を超えた連携が容易になる
- **可視化・説明責任の明確化：**内部統制評価の結果、検出された問題点を集約し、どこの拠点に問題点が生じており、担当者の割り当てとその対応状況（ステータス）をレポートなどによって可視化し、コンプライアンスに漏れがない

か一目で把握することが可能になる
- **情報資産の安全性の確保：**ユーザー別にアクセス権を識別し管理することで、企業もしくは企業グループにとって重要な情報を必要なユーザーに限定することが可能になる

たしかに一見すると、プラットフォームが共通化することでこれらのメリットをすべて享受できるように思えます。しかし実際にはGRCツール／システムを導入後に、こうしたメリットを享受できていない組織も少なくありません。このような組織の原因分析をしてみると、GRCツール／システムの導入目的や利用者のITリテラシーといった導入チームで解決可能な領域を超えた、全社的なITガバナンス・データガバナンスの問題が根幹であることが少なくありません。そこで、先ほど挙げたGRCツール／システムの5つのメリットを得るための前提条件を見てみましょう。

- **情報の一元化：**対象システムで必要な情報、情報の形式、情報の更新頻度といった「データガバナンス」と呼ばれる原則を明確にしたうえで、誰がどうやってこれらの情報を収集・更新・利用するのかを決めていること
- **業務の標準化と効率化：**業務そのものの標準化が完了していること。標準プロセス以外の業務プロセスを経る場合の例外措置が決まっていること
- **業務の自動化：**自動化のスタートとなるアクション、アウトプット、これらのアクションの責任者が明確なこと。エラー検知の仕組みが存在していること
- **可視化・説明責任の明確化：**リスクの責任者が明確で、誰にリスク対応を割り当てればよいのか全社の体制が定まっていること。リスクの対応状況をモニタリングする責任が明確でモニタリング担当者に一定程度以上のITリテラシーがありツールによるモニタリングが実施できること
- **情報資産の安全性の確保：**対象システムで必要な情報に求められる機密性、完全性、可用性が明確かつ、これらのセキュリティ要件を満たすために求められるシステム要件が定まっていること

これらの前提条件はいずれも内部監査部門単独では解決が困難な、全社のDX戦略との調整が必要な事項です。これらの前提条件が未解決のままであったとしても、GRCツール／システムを導入し、機能の一部を活用することで、部分的にこうした期待効果を達成することは可能ですが、比較的高額となりやすい投資に見合った効果は得られない可能性があります。

このように、共通プラットフォームとしてのGRCツール／システムは、決して内部監査部門や内部統制部門単独で導入をして成功裏に収められるものではなく、全社のITガバナンス・データガバナンス戦略の下でのみ実現可能なのです。

3 ステップ3：それでもGRCツール／システムを導入すべきか？

前述のとおり、GRCツール／システムの導入効果を享受するためには、全社的なITガバナンス・データガバナンスの整備が欠かせません。では、内部監査業務や内部統制業務の効率化・高度化は、こうした全社的な活動を待たなければできないかというと、必ずしもそのようなことはありません。GRCツール／システムの導入パタンとしては、次の2つが考えられます。

- **パタン1：**GRCツール／システムの導入プロジェクトを通して全社のデータガバナンスの整備を進めながらDXを推進する
- **パタン2：**GRCツール／システムの特定機能・モジュールを活用して部分的にDXを推進する

GRCツール／システムの導入については、パタン1が実現できれば理想的です。ただし、調整が必要なステークホルダーが多く、相応のコストが必要になります。そのため、次善の策としてパタン2を選択する組織も多く見られます。得られるメリットが限定されることを承知したうえでの投資であれば、この選択肢も悪くありません。しかし、そもそもの「GRCツール／システムによる統合管理」という目的を達成することができないのであれば、既存の社内ツール／システムを活用して、部分的に業務効率を上げることができないかどうか検討するほうがより効果的です。

4 ステップ4：あなたの組織は本当にGRCツール／システムを導入していないのか？

ここまでGRCツール／システムと呼ばれるソリューションのモジュールやメリットについて確認してきました。これらのモジュールや役割を1つ1つ確認すると、それぞれをサポートする情報システムは社内にすでに存在していることに気がつきます。そこで**図表5**に、多くの組織ですでに使われていることが多い社内ツール／システムをGRCツール／システム

に転用した例を示します。

トータルプラットフォームとしてのGRCツール／システムのメリットを享受することが難しい、あるいは全社としてのデータガバナンスの整理が進んでいない段階では、社内に既存ITツール／システムを活用して内部監査・内部統制業務のDXを推進し、そのあとで段階的にGRCツール／システムの導入に取り組むという方法もあります。

以下に、既存システムを活用しながらGRCツール／システムを導入した事例を示します。

- **事例1：**情報システム部門がITヘルプデスク業務で利用をしていた問合せ管理システム（インシデント管理にチケットシステムを使用）を内部監査部門でも利用し、監査の指摘事項のモニタリングに転用。ITガバナンス・データガバナンスの成熟度と平仄を合わせて、このチケットシステムのモジュールが含まれるGRCツール／システムパッケージを導入。
- **事例2：**全社で導入済みのクラウド型オフィスアプリケーションソフトのアンケートフォームとファイル共有の仕組みを利用して、内部監査の予備調査項目の配布、被監査組織との情報のやり取りを実施。内部監査部門、被監査組織双方がオフィスアプリケーションによる内部監査に慣れてきたタイミングで、このオフィスアプリケーションとユーザーインターフェイスが類似したGRCツール／システムの導入を通じてデータガバナンスの向上プロジェクトを開始。
- **事例3：**内部監査の際に活用してきたリスクシナリオを、全社で導入（予定）のデータビジュアライズプラットフォームを活用したダッシュボードでビジュアライズ化し、内部監査とコンプライアンス部門のメンバーがダッシュボードを活用できるようにトレーニング。データからのリスクの読み取りが得意なメンバーを選抜し、データガバナンスプロジェクトを組成。このチームが情報システム部を支援して、全社のERP入れ替えプロジェクトの中でデータガバナ

図表5：既存社内ツール／システムの内部監査・内部統制活動への転用例

社内ツール／システム	内部監査・内部統制活動への転用例
バージョン管理支援ツール	コンピュータプログラムや契約書のように、正確なバージョン管理が求められるファイルの管理を行うための支援ツール。監査プログラムや監査調書のバージョン管理に転用可能
プロジェクト管理支援ツール	大規模プロジェクトを管理する際のプロジェクト支援ツール。年度監査計画から個別監査計画に落とし込む際の工数管理、スケジュール管理、個別監査の進捗の管理といった内部監査部門長、監査リーダーのモニタリング業務に転用可能
インシデント管理（チケット管理）ツール	ITヘルプデスクや人事部門の相談機能のように社内の多くの方から来る雑多な相談事への対応を取りこぼしなく、優先順位をつけて対応するための支援ツール。IT端末等へのパッチの自動適応等の機能を有するものもある。被監査組織とのコミュニケーション、指摘事項の管理、指摘事項に対する改善状況のモニタリング等に転用可能
ワークフロー管理ツール	稟議決裁の承認申請等を行うためのワークフローシステム。主に1つ上のインシデント管理ツールと同じだが、ITとの自動連携機能はないことが多い代わりに職務権限との連携が強いことが多い
データ分析支援ツール	内部監査におけるデータ分析をもとに機能を拡充したCAATs（Computer Assisted Audit Techniques：コンピュータ利用監査技法）と呼ばれるものや、ETL（Extract、Transform、Load）ツールと呼ばれるデータの分析専用プラットフォーム等。内部に簡易的なデータベースを持ち、データレイク的に活用できるものと、純粋な分析機能だけのものがある。一般的には前者を「GRCツール」や「ETLツール」と呼び、後者を「CAATsツール」と呼んでいる
データビジュアライズ支援ツール	データ分析支援ツールやデータビジュアライズツール。データ分析や各種管理状況を視覚的にわかりやすくグラフや表にするために利用することができるため、内部監査の予備調査としてダッシュボード化や、リスクアセスメントの結果のビジュアライズ等に活用可能
オフィスアプリケーション（アンケートフォーム）	クラウド型のオフィスアプリケーションに包含されているアンケート作成・回収フォーム。多数の回答者に同一の質問を送信・アンケートフォームで回収をすることができるため、リスク分析や内部通報の受付等に転用可能
オフィスアプリケーション（表計算ソフト）	データ分析やデータビジュアライズを目的として汎用的に利用されている表計算ソフト。データ分析やデータビジュアライズ、プロジェクト管理等に活用できる。クラウド型のオフィスアプリケーションに包含されている表計算ソフトの場合には、アクセス権を適切に設定することで全社のリスク分析のプラットフォームやインシデント管理、内部南沙の指摘事項のモニタリングツール等にも転用可能
基幹システム（ERP）のGRCモジュール	ERPパッケージで取り扱うデータに対して、GRC領域でモニタリングすべきスレッシュホールド（閾値）等を設定して異常点のアラートを出すためのダッシュボードや、閾値を設定するための機能を拡充したモジュール。他の既存ツールとは異なり部分的な活用は難しいが、データガバナンスを整理しながらトータルプラットフォームとして活用することができれば効果は高い

ンスの成熟度を向上させ、ERPシステムのGRCモジュールの一部を導入。

5 ステップ5：GRCツール／システムを成功裏に導入可能な経営を求める

ここまで読まれてきて、「うちはまだGRCツール／システムの導入は時期尚早」と思われる方もいらっしゃるかもしれません。時期尚早だとは思うのだけれども、全社的にDXを推進していて、内部監査・内部統制部門でも同様の取り組みが求められている組織もあるでしょう。このような場合には、コストの高いGRCツール／システムをリスク管理のプラットフォームとして導入する前に、既存の社内ツール／システムを活用できないか検討するのも有効な策となります。

一方で、データ活用を推進して組織としての競争力を高めるためには、データガバナンスの成熟度を高め、GRCツール／システムを有効に活用できる組織になる必要があると感じていた方もいらっしゃるのではないでしょうか。GRCツール／システムは本来、特定の部門の業務改革や業務の効率化のために導入されるものではなく、経営全体の質を向上させるためのツールです。内部監査部門であればデータガバナンスの成熟度について内部監査を実施したり、内部統制部門であれば全社および部署別のDXの推進度合いや、事業戦略の達成度についてリスクアセスメントを行うなどの統制活動を通じて自社のDXを支援することができます。

また、トップマネジメントがこのような内部統制活動や内部監査活動を要請することは、統制の強化とDXの推進の両面から有効と考えます。

岩永 摩美（いわなが あみ）
PwCあらた有限責任監査法人
ガバナンス・内部監査サービス部　ディレクター
アドバイザリーファームにてリスク管理体制の高度化および情報セキュリティ体制支援に従事後、テクノロジー系事業会社の内部監査室長および海外子会社の監事として内部統制の強化や不正調査に従事。デジタル関連領域の幅広い知見と技術をもとに、テクノロジーを活用した内部監査や内部統制の高度化支援に従事。
メールアドレス：amy.iwanaga@pwc.com