Ridgelinez

DXを実現するための デジタルリスクマネジメントの要諦

DX時代のリスクマネジメント
トランスフォーメーション

Table of Contents

注 1. DRM: デジタルリスクマネジメント

はじめに

このレポートは、「DX 施策におけるリスクマネジメントの取り組み状況」に関する調査結果の考察を通して、Ridgelinez が考えるデジタルリスクマネジメント（以下 DRM）のあるべき姿を提言するものです。本調査の考察は、売上高 1,000 億円以上の企業で、DX 推進におけるリスクマネジメントに関与している課長職以上の方 950 名を対象にしています。

今回、企業の DXプログラムにおけるリスクマネジメントの実施状況や課題についてアンケートを行い、DRMの実態を把握すると共に、DRM の成熟度による違いを考察しました。調査結果に基づく分類からは、DRM の成熟度の高い企業は全体の 15％にとどまり、成熟度の低い企業が 74％という結果となりました。DRM の成熟度が高い企業ほど DXプログラムの進捗が順調となる傾向があり、DXプログラムの進捗と DRM の成熟度には相関関係がみられました。

今回の調査結果から、約 4 割の企業が「DRM を後回しにすると DX が停滞しかねない」と認識しており、今後 DRMの体制構築は必須と考えていることがうかがえます。DX が浸透することにより、テクノロジーリスクとビジネスリスクが混在し、対応すべきリスクは多岐にわたります。今後 DX をさらに推進するためには、全社的かつ横断的な DRM を整備し、DX の信頼性を確保することが肝要です。

Chapter 01

企業を取り巻くリスク環境とDXプログラムの関係

デジタル化によるリスク環境の変化

DX への取り組みが待ったなしとなる中、リスクマネジメントへの取り組みの難しさが明らかになってきています。セキュリティインシデントを例に見てみると、2019 年度の原因究明に関する費用や改善策の導入、損害賠償等事後対応を含めた被害総額（年平均）は約 1 億 5,000 万円というデータもあります。[注2]

近年では、データ保護リスク、事業継続リスク、倫理リスク、クラウドリスクなど多岐にわたるインシデントが頻発しています。一方で、GDPR[注3] や NIST SP800-171[注4] などデジタル関連の国際的なレギュレーションやガイドラインなどのルール策定が進んでおり、日本国内でも追随する動きとなっています。

デジタル化によるリスク環境の最も重要な変化は、企業として守る経営資源が“システム”に加えて、“データ”まで拡がることにあります。

個人情報のデジタル化や IoT、AI の利用拡大により、データの爆発的な増加に加えて、データ自体の価値が高まることで、それらデータの機密性や完全性、可用性が毀損されることによるビジネスへの影響は著しく大きなものとなっています。また、IoT や AI により生成されるデータに関しては、本当に信用できるのか？という“真正性”のリスクについても考える必要が出てきています。デジタル社会、データ駆動型社会において、データの安全・安心・品質の確保は企業経営にとっても重要なテーマとなっていることは明らかです。

また、デジタル化の流れにおいて、パブリッククラウドの活用も前提となっており、英国や米国ではすでに政府調達においてクラウドファーストを掲げたうえで、クラウドサービスの認証制度を導入するなど、パブリッククラウドの採用は世界的な潮流になりつつあります。日本でも 2018 年に「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において、“クラウド・バイ・デフォルト原則”を採用するとともに安全性評価の仕組みを検討し、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用が開始されています。

これらクラウドサービスに係る認証制度や安全性評価の議論は、一方でクラウド活用における新たなリスクを示唆しています。SoE（System of Engagement）などでは現場部門主導でパブリッククラウドを導入するケースが増えていますが、これらのケースでは、IT 部門がクラウドリスク対応に関与できないために設定ミスが解消されず、脆弱性として残り続けるリスクが散見されています。

もう 1 つ、DX 推進においては、“つながるリスク”に留意する必要があります。つながるリスクは、外部プレーヤーやサプライヤーと構築するデジタルエコシステムに伴うものと、IoT の活用によるサイバー空間とフィジカル空間の融合に伴うものの 2 つがあります。
デジタルエコシステムの形成では、パブリッククラウドやオープン API の活用により、パートナーやサプライヤー、顧客とつながることで新たなビジネスモデルの構築やバリューチェーンの再構築が可能となります。
しかし、デジタルエコシステムの連携先にセキュリティレベルが低いプレーヤーが存在することで、そこをターゲットに攻撃され、他のプレーヤーにまで被害が波及することになります。DX において外部連携は不可欠であり、ビジネス機会を拡大するための必須要件ですが、同時にリスクを増大させる施策でもあるため、十分なリスク評価とセキュリティ対策により、デジタルエコシステムのセキュリティの“桶の高さ”を揃えることが重要です。

注 2. 出所：トレンドマイクロ 法人組織のセキュリティ動向調査 2020 年版 https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201002-01.html
注 3. General Data Protection Regulation: EU 一般データ保護規則。EU で 2018 年より施行されている個人情報（データ）の保護に関する規則。 行政罰規定があり、違反行為に対しては、高額の制裁金が課されるリスクがある。
注 4. 米国国立標準技術研究所（NIST: National Institute of Standards and Technology）が発行するセキュリティガイドライン。このガイドラインでは、機密性の高い重要情報の保護に必要となるセキュリティ要件がまとめられている。米国国防総省の調達規則（DFARS: Defense Federal Acquisition Regulation Supplement）では、「CUI（Controlled Unclassified Information）」と呼ばれる管理すべき重要情報を取り扱うサプライヤーに対し、当該ガイドラインへの準拠が 2017 年より義務化されている。

海外におけるデジタルリスクのインシデント発生事例

データ保護リスク

不適切な情報の取り扱いによる情報流出

（豪州軍需関連企業の事例）兵器に関する重要情報が、ハッキングによって同社のサプライヤーから窃取。防衛産業の多層化、グローバル化が進む中で、防衛製造大手ではサイバーセキュリティ対策が進められる一方で、中小規模のサードパーティに潜むリスクが露呈。

事業継続リスク・サプライチェーンリスク

生産システムのウイルス感染

（欧州金属生産会社の事例）生産ラインに IT システムを導入したが、フィッシングメールによってシステムがウイルスに感染。40 カ国の事業所に次々と感染が拡大したため、社内ネットワークを遮断し、全コンピュータを停止。その結果、手動操業できない一部の工場で生産が停止し、数十億円規模の金銭的損失が発生。

倫理リスク

AI データの偏りによる人権侵害

（米国ネット通販会社の事例）人事部門の負荷軽減や応募者と企業とのミスマッチの減少を目的に人材採用 AI を導入。しかし、機械学習させるためのデータに偏りがあり、「女性」という言葉が履歴書に記載されていると応募者の評価が下がってしまう結果となり、男女の人権問題に発展しかねない事態となった。公平性を欠いた男女差別につながると判断し同サービスの活用を終了。

クラウドリスク

脆弱性による不正アクセス

（小売会社の事例）自社の小売サービスと連携させたオンラインカード決済のためのクラウドサービスを開始。既存ビジネスとのシナジー効果を期待し、CX（顧客体験）の向上を図った。しかし、脆弱性による多数の不正アクセス・不正使用がリリース開始とともに相次ぎ発覚し、最終的にはオンライン決済サービスから撤退。

レギュレーション・ガイドライン違反リスク

新たなガイドラインに違反

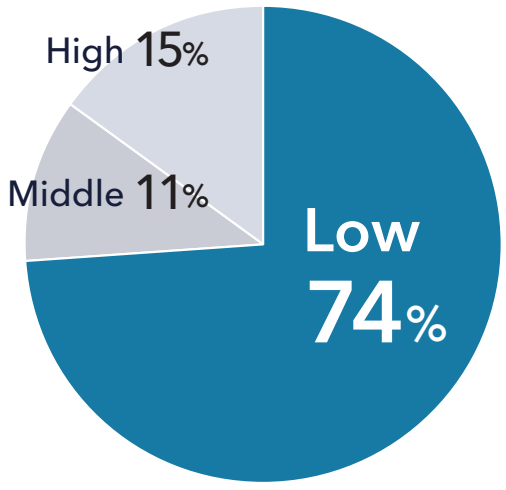
（英国航空会社の事例）不完全なセキュリティ対策が原因で、氏名や住所、カード決済や予約内容含む約 50 万人の顧客データが流出。欧州一般データ保護規則（GDPR）の違反として、同社に対し、日本円にして約 2,500 億円超ものペナルティが科された。

サイバー空間とフィジカル空間の融合では、現場から収集したデータをサイバー空間で分析、フィードバックすることで、フィジカル空間における現場作業の高度化が可能となります。
しかし、IoT が導入される工場系や制御系のネットワークは、これまでクローズドなネットワークとして運用されてきたため、オープンな環境に耐えられる構造になっていません。つまり、オープンなネットワークとつながることで、それまで露呈していなかった脆弱性が狙われることになります。さらに情報システムの停止とは異なり、サイバー攻撃により設備の稼働そのものが停止するなど、影響はフィジカル空間にまで及び、場合によっては重要産業や重要インフラのオペレーションまでもが停止し、国民生活の安心安全を脅かすことにもなりかねません。

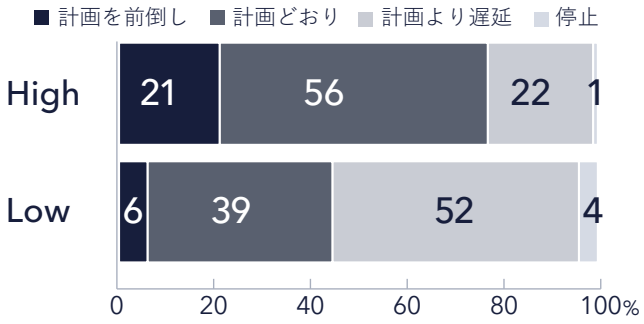
DXの進捗度合いとDRMの関係

今回、Ridgelinez では、DX を通じて変革を遂げるには DX におけるリスクマネジメント（デジタルリスクマネジメント、以下 DRM）を実践することが最重要課題の 1 つであるという仮説に基づき、DX 推進経験者を対象としたインターネットモニターリサーチを実施しました。本調査では、DX 推進経験がある方に、自社の DX への取り組み状況と DX 推進時のリスクマネジメントについて尋ね、DX プログラムにおけるリスクマネジメント（DRM）の成熟度別に傾向を分析しました。
成熟度については、リスク評価、対応策の検討・優先順位付け、ロードマップ策定、施策実行とモニタリングのプロセスの実施状況に基づいて 3 段階（High, Middle, Low）に分類し、結果 High と評価できる企業はわずか 15% にとどまりました。一方で、74% の企業は Low に分類される結果となりました。

【図表 1】DRM マチュリティレベル



【図表 2】DRM マチュリティレベル別 DX 進捗状況



さらに、DRM の成熟度別に DX プログラムの進捗状況をみると、DX プログラムは、DRM の成熟度が High の企業ほど計画どおりに進んでおり、成熟度が Low の企業では、遅れや停滞が目立つ傾向が明らかになりました。これらの結果から DX の進捗と DRM の成熟度には一定の相関関係があることが推察できます。一方で、国内企業の DRM に対する取り組みは進んでいないことがうかがえます。
以降、調査結果をもとに DX プログラムにおける DRM の現状や課題、経営インパクトに対する理解について考察していきます。

Chapter 02

DX企業が目指すべきDRMとその現状

DX企業で目指すべきDRM

DXで対応するべき4つのリスク

DX プログラムで対応が必要となるリスクは、DX の特性から大きく 4 つに分類することができます。

データ保護リスク

パブリッククラウドや API 技術などの活用による企業内･企業間のデータ流通が今後加速することで、データが脅威に晒される機会が増えるため、デジタルエコシステム全体でセキュリティやプライバシーのリスクへの対応が必要になります。

ビジネスモデル変革リスク

DX によるビジネスモデル変革では、従来の延長線上にないビジネス環境や時には業界を超えた環境に進出するため、新しいルールやセキュリティリスクを特定･評価したうえで、リスクコントロールの実装やモニタリングを行うことが不可欠です。

新技術適用リスク

AI や IoT、5G などの新技術適用の際は、新たな脆弱性や未知の脅威に晒されるだけでなく、リスク発現によるビジネスインパクトも計り知れないため、必ずリスク評価を実施するだけでなく、レジリエンス向上への取り組みも重要です。

プロセス変革リスク

RPA や AI 等のデジタルレイバー[注5] 導入による自動化などでは、デジタルレイバーに適切に指示されないリスクや関連システムの変更が連携されないリスク、不正アクセスなど、従来システムと同様に IT 全般統制による対応が求められます。

注 5. デジタルレイバー：仮想知的労働者。人の代わりに知的労働を行うソフトウェア全般を指す。

DXのリスクマネジメントプロセス

このリスク分類に基づきデジタルリスクを抽出・整理した上で、リスクマネジメントを運用することがDX企業にとっての必須課題です。

① DXプログラムのリスク評価
↓
② 対応策の検討・優先順位付け
↓
③ ロードマップ策定
↓
④ プログラム実行
↓
⑤ モニタリング

具体的には、DXプログラムごとに①業種や施策内容に応じた観点でDXプログラムに係るリスクの特定と評価をDX推進部門が自ら行い、②リスクへの対応策の検討と優先順位を付けたうえで、③各対応策のオーナーのアサイン、アクションアイテムの棚卸、スケジュールへの落とし込みなどのロードマップ策定を実施します。
ロードマップ策定後は、④プログラムを実行し、⑤モニタリングによりプログラムの実行状況や課題などを把握します。
このようなプロセスを運用することにより、DXプログラムの初期段階でリスク認識をしたうえで、リスクコントロールを日常的に行うとともに、有事に備えてレジリエンスを高めていくことが可能になります。

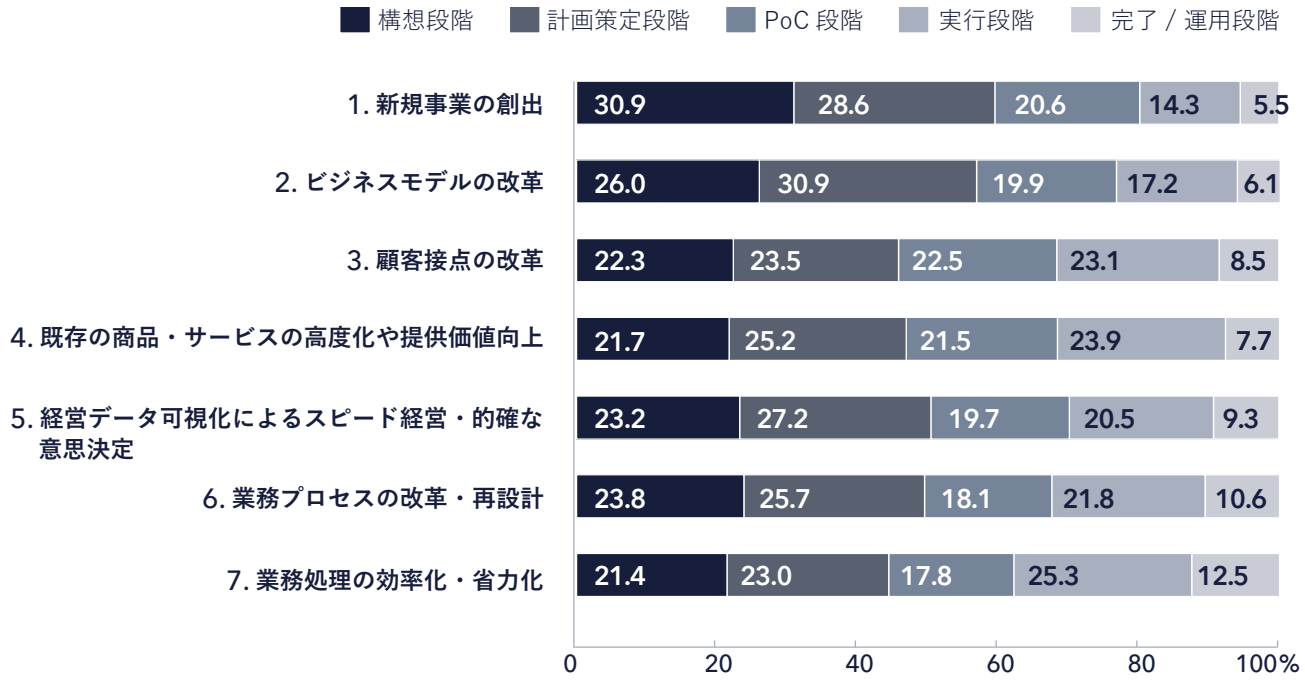
DXプログラムとリスク認識の現状

前述の目指すべきDRMの仮説検証として今回のリサーチ結果からDXプログラムとリスク認識の現状をみていきます。

DXプログラムへの取り組み状況

DXプログラムの進捗状況はいずれも「構想・計画段階」のものが多いことがわかります。「5. 経営データ可視化によるスピード経営・的確な意思決定」、「6. 業務プロセスの改革・再設計」、「7. 業務処理の効率化・省力化」など、従来の延長線上にある取り組みについては、比較的に“実行段階”以降が多いようです。

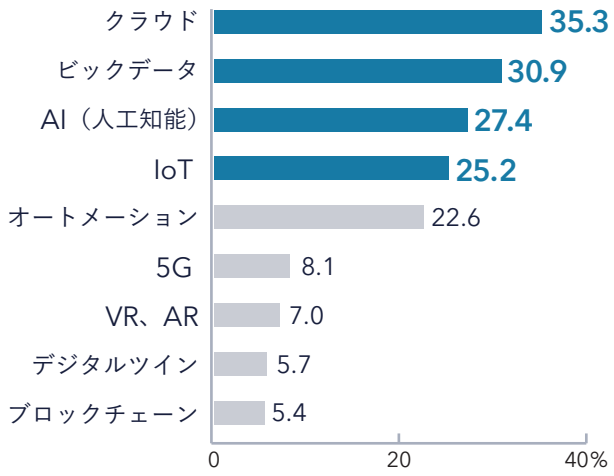
【図表3】DX施策への取組み状況



次に DX 施策別に活用されているテクノロジーの傾向を見てみると、クラウドやビッグデータ、AI、IoT などが各施策で幅広く活用されていることがわかります。5G やデジタルツイン[注6]、ブロックチェーンなどは現状の活用状況は進んでないものの、今後は活用拡大を見込んでおく必要があるでしょう。

注6. デジタルツイン：フィジカル空間（現実世界）の情報をリアルタイムに収集しデジタル空間に送信して、フィジカル空間と同じ環境をデジタル空間に再現する技術。双子（ツイン）のように連動させることで高度なシミュレーション等を行うことが可能。

【図表4】施策毎の活用テクノロジー



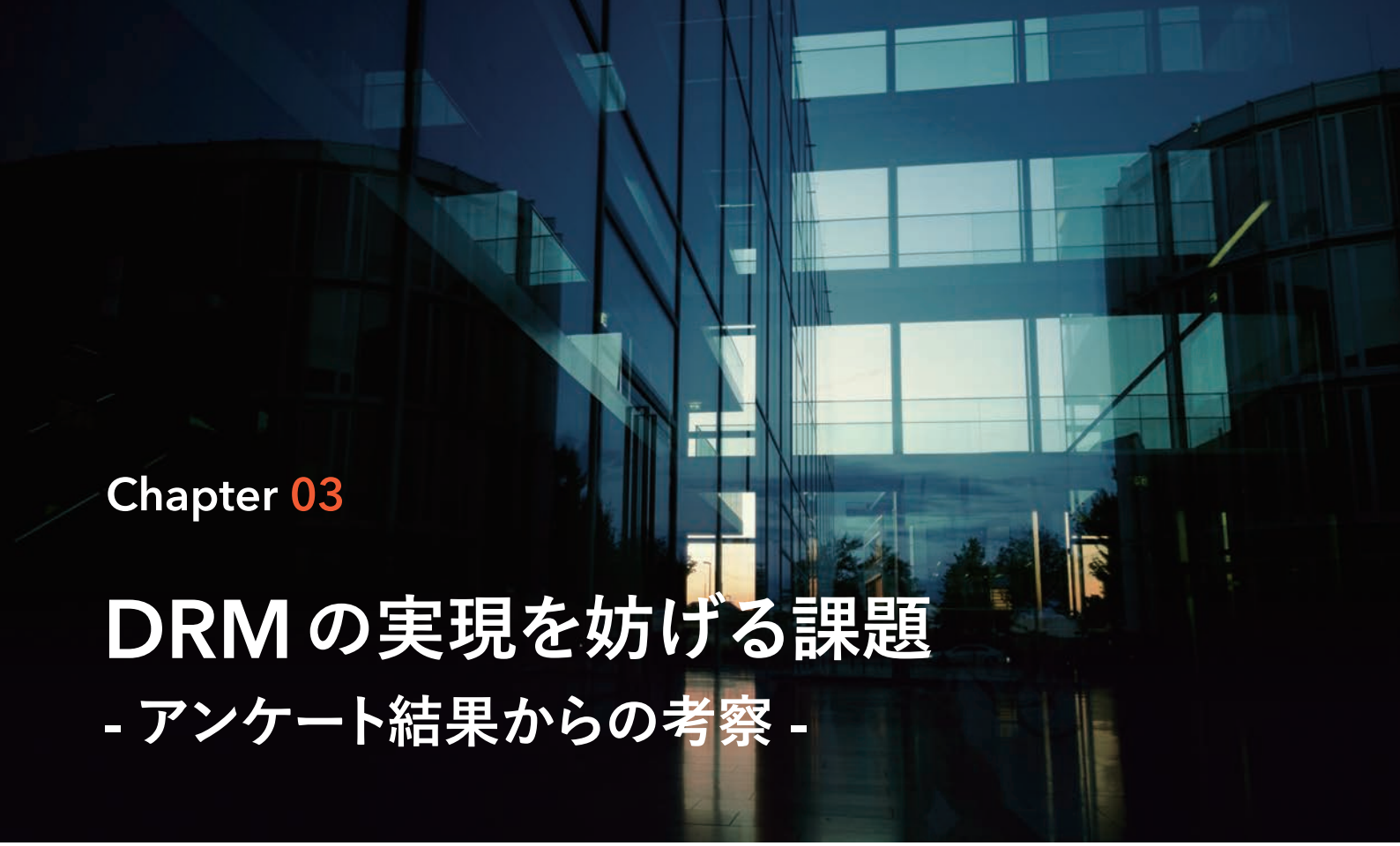
DXプログラムにおいて重視するリスク

このような DX プログラムの取り組み状況の中で、最も重視されているリスクは、データ保護リスクやクラウドリスクといったテクノロジー関連のリスクであることがわかりました。一方で、レギュレーションリスクや倫理リスク、事業継続リスク、サプライチェーンリスクなどのビジネス関連のリスクについては、認識が低い傾向もわかりました。

【図表5】DXプログラム毎に最も重視するリスク

	クラウドリスク	データ保護リスク	プライバシーリスク	レギュレーション・ガイドライン違反リスク	倫理リスク	生産性低下リスク	ビジネス変革リスク	事業継続リスク	サプライチェーンリスク
1.新規事業の創出	20.1	22.2	11.1	6.3	3.4	4.5	13.5	9.2	2.6
2.ビジネスモデルの改革	13.6	19.5	14.4	8.5	2.8	6.6	19.5	6.6	2.8
3.顧客接点の改革	10.8	23.6	26.5	7.0	5.0	5.8	8.7	5.0	2.0
4.既存の商品・サービスの高度化や提供価値向上	11.5	18.9	12.7	7.4	4.4	12.1	13.3	8.6	4.1
5.経営データ可視化によるスピード経営・的確な意思決定	10.8	23.6	12.4	8.0	6.0	9.2	12.8	8.0	2.8
6.業務プロセスの改革・再設計	6.2	18.6	8.1	9.1	4.1	21.5	11.9	7.6	4.1
7.業務処理の効率化・省力化	7.3	19.7	6.7	8.1	2.0	23.6	14.9	6.5	2.2

DXプログラムが多くの企業で構想・計画段階にあることに加えて、DX関連リスクが多岐にわたることから、DX初期のPoCで直面するリスクや机上で想定できるようなリスクについては、認識されていますが、DX本格期に直面すると想定されるようなコンプライアンスリスクや、ビジネスリスクに対する認識が十分でないということが、これらのデータから推察できます。



Chapter 03

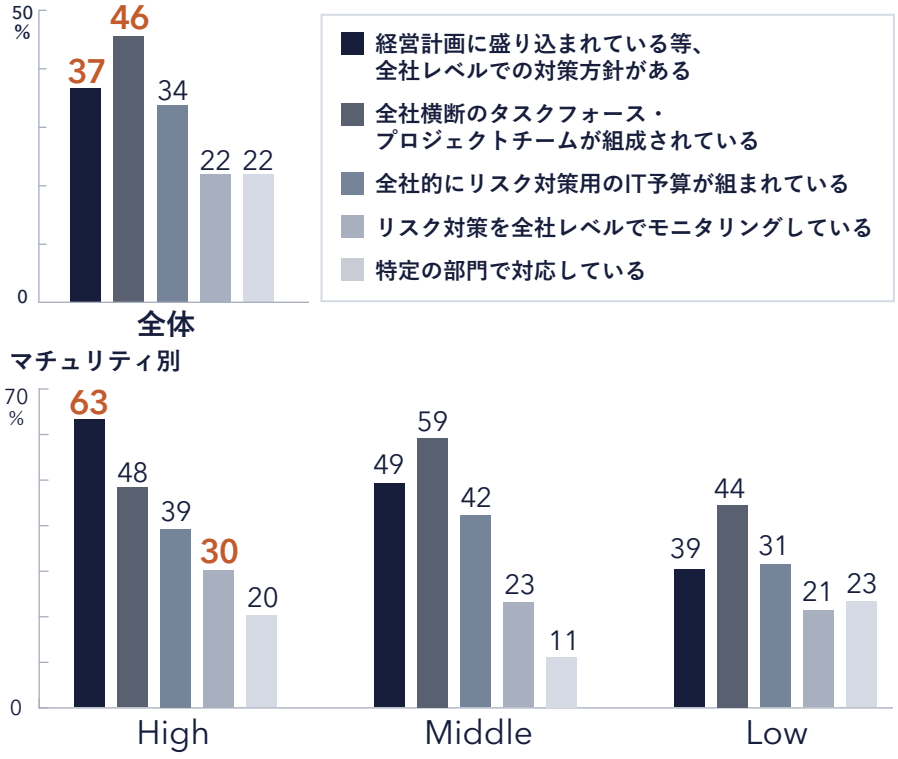
DRMの実現を妨げる課題
- アンケート結果からの考察 -

企業におけるDRMの実態

全社レベルでの取り組み状況

Q9 「Q9. DX 施策 におけるリスク対策に関して、全社レベルでどのような取り組みがありますか？」という設問では、以下のような回答結果となりました。

【図表6】全社レベルでの取組み状況



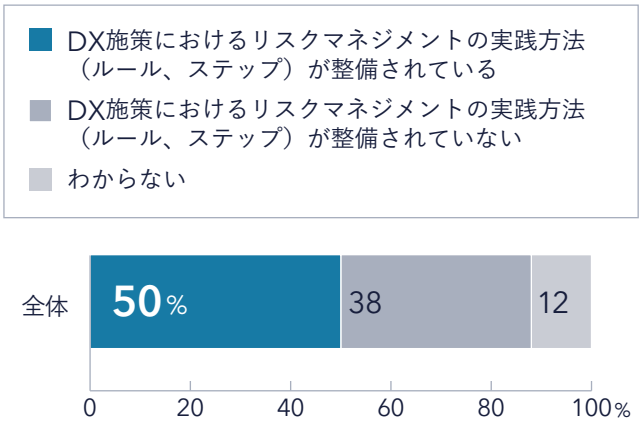
DRM に関して、「全社横断のタスクフォース・プロジェクトチームが組成されている」（46%）、「全社レベルでの対策方針がある」（37%）など、ある程度経営レベルでの対応が進んでいる状況とみることもできますが、いずれの設問でも 50%を切る結果からは、多くの企業で経営も関与する全社的な DRM の取り組みを今後の重点課題と考えるべきだということが言えるでしょう。

また、成熟度が High の企業では、「全社レベルでの対策方針がある」（63%）、「全社レベルでモニタリングしている」（30%）が相対的に高くなっており、持続的な DRM の実践においてこの 2 つの取り組みは重要であると言えます。

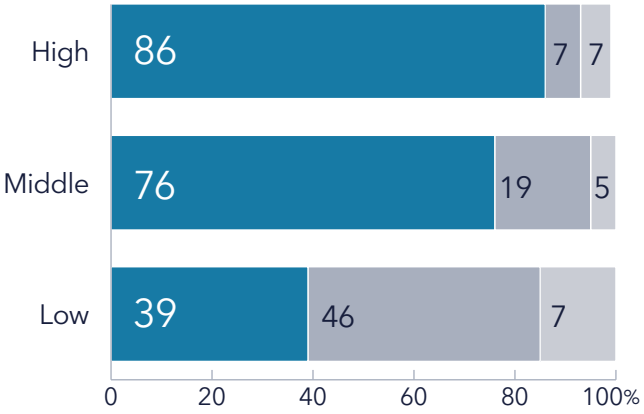
実践方法の整備状況

Q10 **次に「Q.10 DX 施策におけるリスクマネジメントの実践方法（ルール）、ステップについて、社内での整備状況として最も近いものを 1 つお答えください」という設問では、以下のような回答結果となりました。**

【図表 7】実践方法の整備状況



マチュリティ別

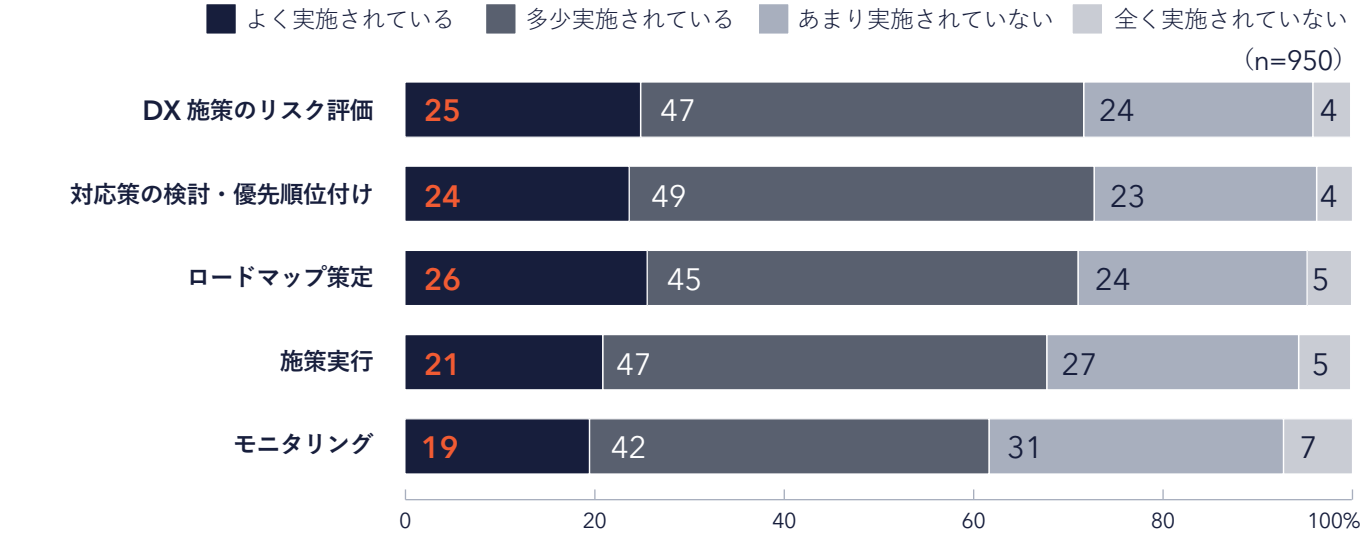


実践方法については全体の半数から「整備されている」という回答が得られましたが、成熟度別では差が出る結果となりました。

成熟度別で見てみると High と Middle は 80% 程度が「整備している」という回答でしたが、Low に至っては 39%にとどまる回答となりました。全体の 4 割弱において DRM の根幹とも言える実践方法が整備されていない実態を示しており、多くの企業が DX 推進に必要な要件を未だ満たせていないことを示しています。

Q13 **さらに「Q13. DX 施策のリスクマネジメントにおける各プロセスの実施状況として、最も近いものを 1 つお答えください。」という設問では、以下の回答結果となりました。**

【図表 8】DRM プロセス実施状況

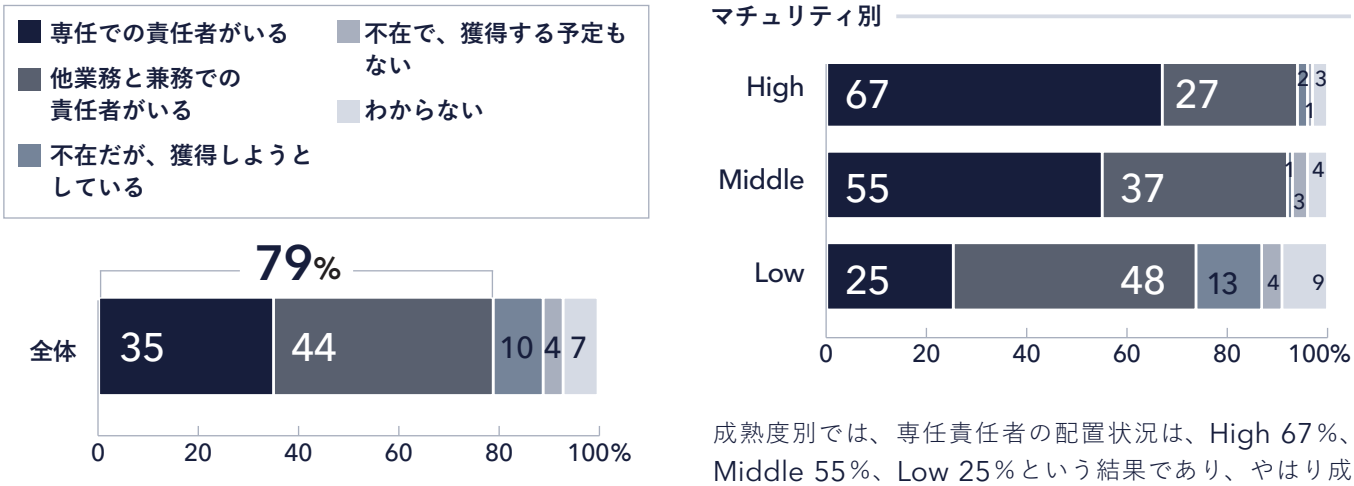


「よく実施されている」の回答は、リスク評価からモニタリングまで、いずれも 30%に満たず、70%の企業で DRM プロセスが運用されていない状況も確認することができました。

DRM 体制

Q11 **最後に「Q.11 DX 施策におけるリスクマネジメントの責任者の在籍状況について、最も近いものを 1 つお答えください」という設問では、以下のような回答結果となりました。**

【図表 9】DRM 責任者の有無



35％で専任の責任者を配置し、44％が兼務の責任者を配置しているという結果となり、（専任・兼任あわせて）約 80％の企業で責任者を配置している実態を確認することができました。

成熟度別では、専任責任者の配置状況は、High 67％、Middle 55％、Low 25％という結果であり、やはり成熟後が高い企業ほど、専任の責任者を配置している状況がわかります。
このように、【図表 7】実践方法の整備状況（50％）と責任者配置の状況（79％）より、DRM の取り組みは責任者の配置から着手している状況がうかがえます。

【図表 10】リスク分類別　対策に関与している部門

	経営企画、DX企画・推進、事業企画	事業部門（製造、調達、営業等）、商品・サービス開発、マーケティング	リスク・コンプライアンス、監査、法務	情報システム、情報セキュリティ	総務、経理・財務、人事	その他、わからない
クラウドリスク	546	422	265	573	182	98
データ保護リスク	556	376	322	620	244	87
プライバシーリスク	485	346	401	522	331	86
レギュレーション・ガイドライン違反リスク	486	343	465	366	209	109
倫理リスク	453	330	490	296	306	105
生産性低下リスク	567	555	146	276	181	102
ビジネス変革リスク	741	497	164	238	186	104
事業継続リスク	718	470	189	252	189	102
サプライチェーンリスク	521	541	166	265	160	132

また、リスク分類別に対策に関与している部門を見てみると、リスクによって関与する部門の傾向は異なりますが、企画部門（経営企画、DX 企画・推進、事業企画）はいずれのリスクにおいても関与率が高い結果となりました。

その他では、データ保護リスク、プライバシーリスク、クラウドリスクなどのテクノロジー関連のリスクは、情報システム・情報セキュリティ部門の関与が高く、生産性低下リスク、事業継続リスク、サプライチェーンリスクなどの

ビジネスリスクについては、事業部門の関与が高いほか、コンプライアンス系のリスクについては、リスク・コンプライアンス部門などの関与が高い傾向が見てとれます。DX はデジタルテクノロジーの活用が前提となるものの、ビジネスモデルの変革では新たなレギュレーションやコンプライアンスへの対応が必要となり、ビジネスプロセスの変革は内部統制の見直しが必要となるなど、複数部門にまたがる幅広いリスクへの対応が求められることがアンケート結果から検証されました。

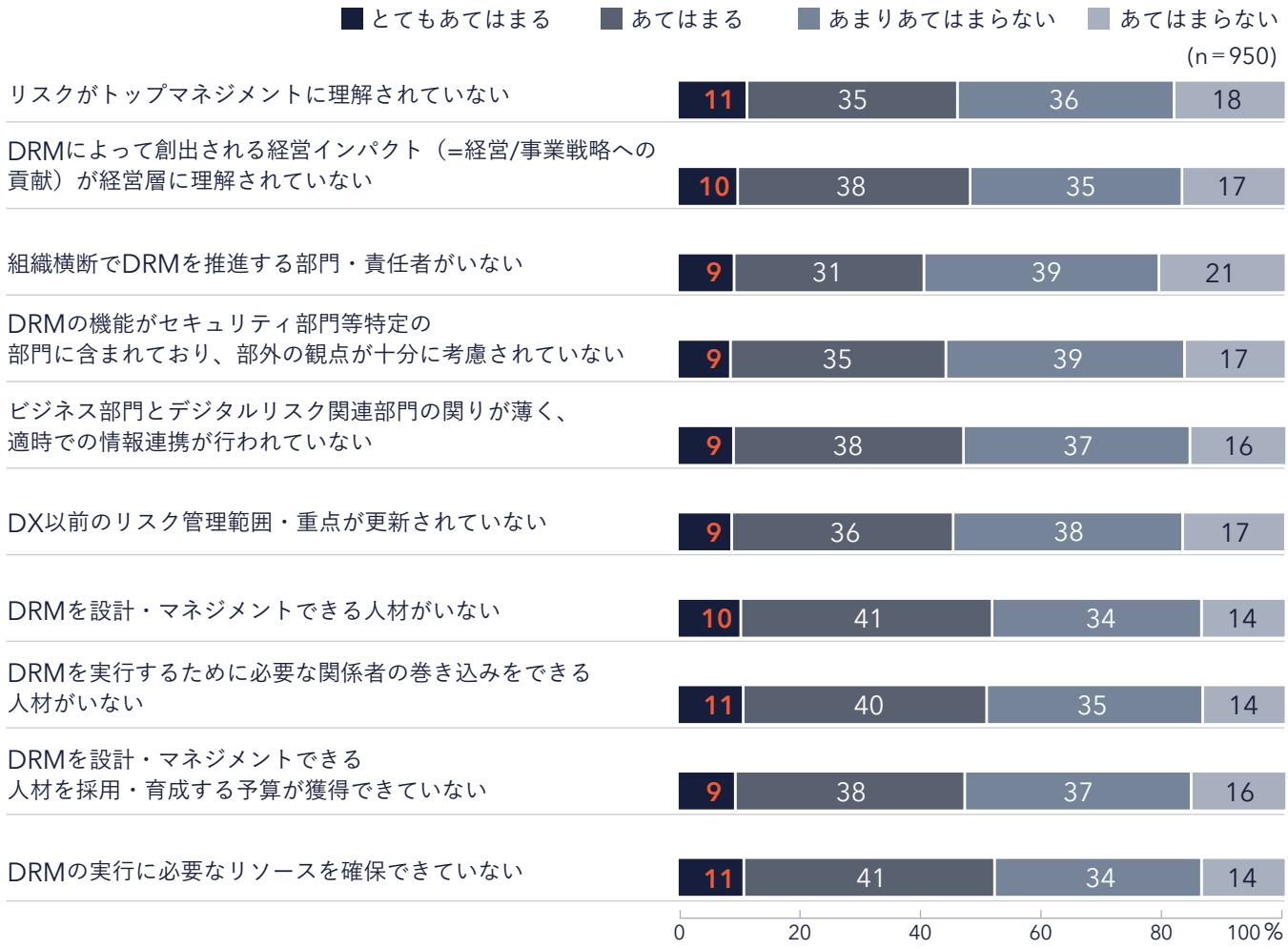
DRMを妨げる課題の認識

Q14 **「Q14. DX 施策におけるリスクマネジメント（デジタルリスクマネジメント）を妨げる課題として、以下の各項目はどの程度当てはまりますか？」という設問については以下のような回答結果となりました。**

主に、「リソースの確保」（52％）、「設計・マネジメントができる人材」（51％）、「関係者を巻き込める人材」（51％）など、リソース全般や人材の不足に関するものが上位に挙がっています。

一方で、「とてもあてはまる」という回答は、すべての設問において 10％前後にとどまっている状況は、全体的に課題認識が十分にされていないのではないか、という懸念が浮かび上がります。

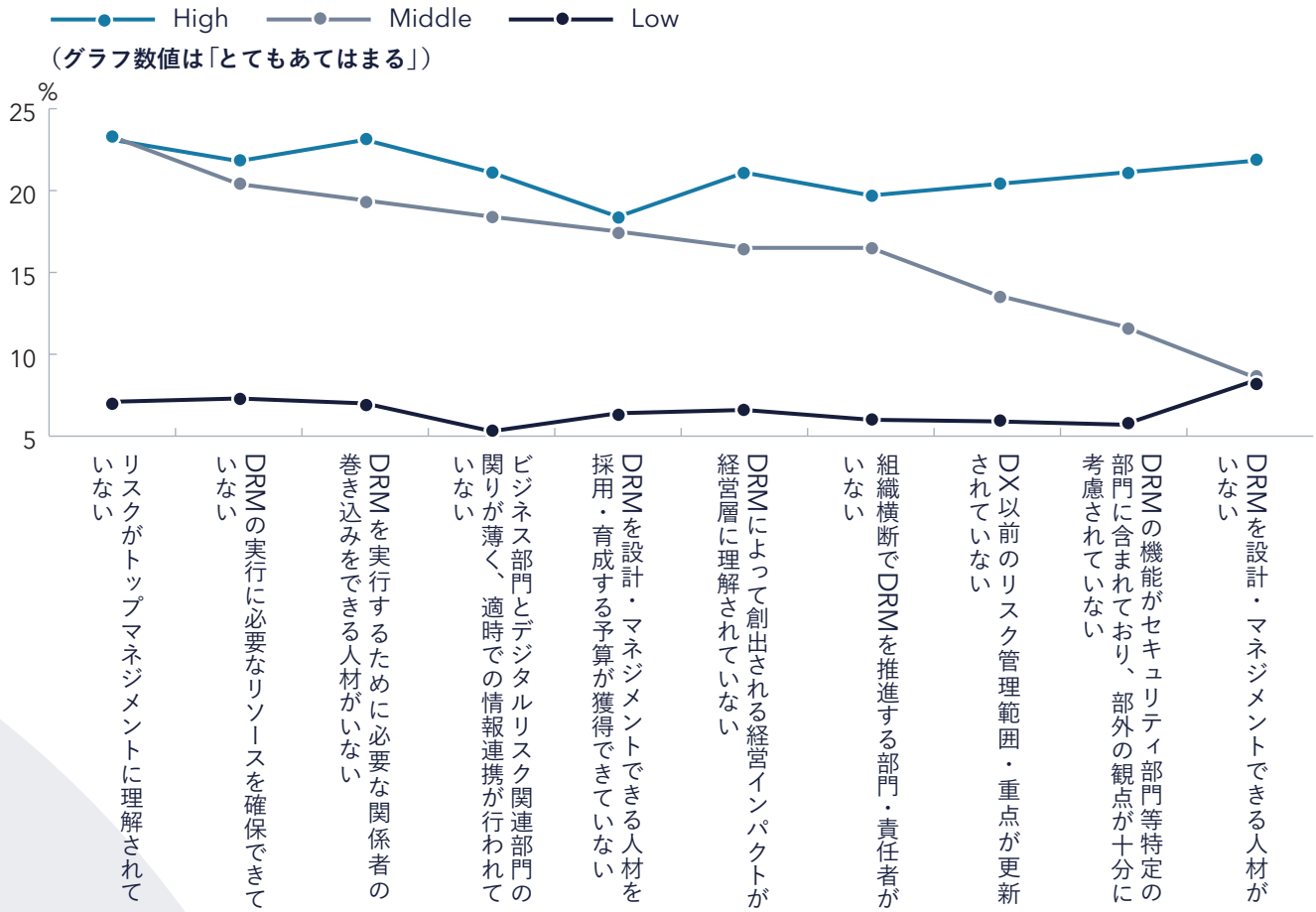
【図表 11】課題認識　全体



「とてもあてはまる」の回答状況を、下図グラフのとおり、成熟度別に見てみると、High の企業が概ね 20％から25％に分布している状況に対して、Low の企業では 5％から 10％に分布しています。この High の企業と Low の企業の差からは、課題認識そのものにも差があることが推察されます。

これは、DX への取り組みがまだ本格的でない中、DRM を妨げる課題も未だ顕在化していないことを示唆していると考えられます。

【図表12】課題認識　マチュリティ別



CASE STUDY

リスク認識と部門協調によるDRM

課題認識不足によるリスク顕在化の懸念

今回のアンケートからは、成熟度が High の企業群がよりクリアに課題認識をしている一方で、成熟度 Low の企業群には課題自体を未だ認識していない企業が多数潜在することが推察されます。

海外における失敗プロジェクトの損失事例

海外では実際にリスク認識の甘さや規制対応への理解不足に加えサードパーティーの管理や選定ミスにより、多大な損失につながる事例も発生しています。

CASE01
移行リスクに対する認識の甘さ

オンラインプラットフォーム移行の失敗により8万人以上の顧客流出

- エディンバラに拠点を置く Trustee Savings Bank（以下 TSB）は、2014 年に旧ロイズ TSB 銀行から分離し、2015 年にスペインのサバデル銀行が買収。
- 2018 年に従来のプラットフォームからサバデル銀行が開発した新しいプラットフォームに 500 万件の顧客口座とデータを移行したが、大規模なシステム障害が発生。
- 数週間にわたりオンラインバンキング・サービスが利用できなくなったほか、その後も数か月にわたり一時的な問題が発生するなど、TSB の信頼が大きく損なわれた。
- 移行プロセスには、13 億件以上の顧客データの移行が含まれていたが、段階的なアップグレードを選択せず、十分な事前テストも行われなかった。
- この障害によるコストは約 3 億 6,600 万ポンド（約 5 億ドル）で、約 8 万人の顧客が他方へ流出。
- ロイズ TSB 銀行時代から TSB を率いてきた CEO も、この事案の責任をとって後に退任するに至っている。

CASE02
規制対応への準備不足

他国事業展開におけるシステム更新でパートナーを選定ミス、9億ドル以上の損失

- ロンドンに拠点を置く電力・ガス供給会社である、National Grid Company は米国北東部に事業進出。
- 2010 年に米国拠点でレガシーの会計管理システムから SAP への更新を決定。
- 当初パートナーとして A 社を選定していたが、後に X 社と Y 社へ変更し、Y 社がシステムインテグレーターを担った。
- プロジェクトは当初から遅延等の問題に直面し、構築されたシステムには欠陥が散見され、従業員への給与支払い間違いやサプライチェーン機能の欠陥により取引プロセスに多大な影響を与えたほか、財務報告の遅れまで引き起こした。
- 損失は 9 億 4,510 万ドルに上ったが、Y 社との訴訟で得た和解金は 7,500 万ドル。Y 社は欧州での経験では豊富であったが、米国が規制するユーティリティ企業に SAP を実装した経験は事実上なかったことが原因とされた。
- 一方で、National Grid 側のプロジェクトに対する準備不足も原因であると、2014 年の National Grid 監査報告書では記載される結果となった。

本格的な DX プログラムの開始に備えて関係部門の協調による DRM の備えをするべき

この 2 つのケースに限らず、DX プログラムにおけるリスクマネジメントの欠落は、ビジネスに直接的な影響を多大に及ぼす可能性が想定されます。さらにアンケート結果からも明らかなとおり、DX プログラムに係るリスクは、従来の IT リスクやセキュリティリスクから拡大、複雑化しており、これらリスクを管理するためには、関係部門が協調的に取り組む必要があります。

本格的な DX プログラムが増えてくる前に、経営層も関与する形で全社横断的な DRM の体制、プロセスの整備と運用に着手するべきではないでしょうか。

Chapter 04

DXの信頼性を確保するためのガバナンスモデル

DXを成功に導くリスクマネジメントの構築に向けて

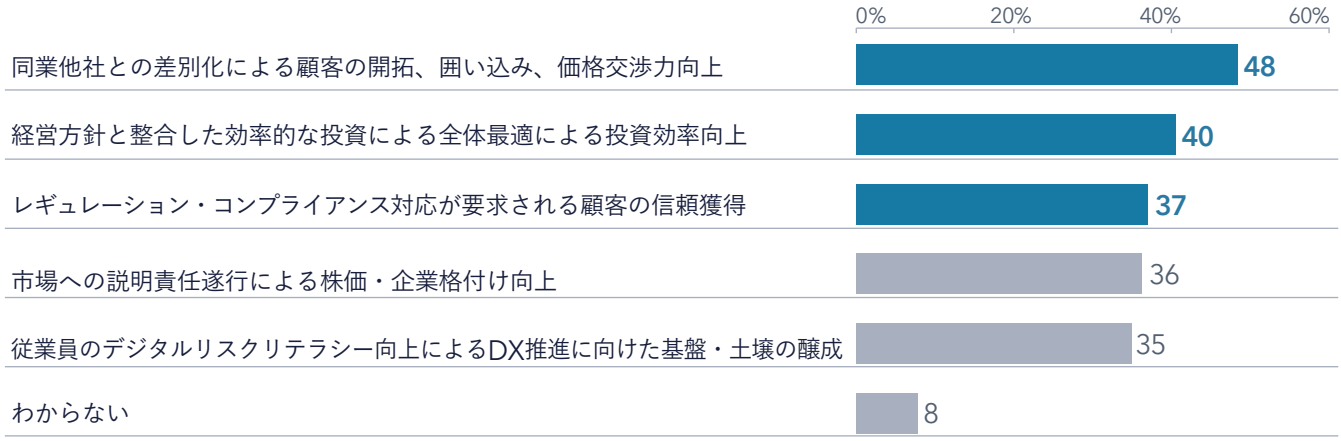
従来型リスクマネジメントからの転換

DRM で扱うリスクは多岐にわたるだけでなく、新しいルールや新しい技術など、未知のリスクへの対応も必要となる。そのため、従来のルールベースアプローチから、リスクベースアプローチによるリスク評価の適切な実施とリスク低減への取り組み、さらにはリスクテイクにおける残存リスクを認識したレジリエンス向上といった DX に適した新しいリスクマネジメントへの転換が求められます。

攻めの経営にインパクトを与えるDRM

Q15 **今回のアンケートでは、「Q15.DX 施策におけるリスクマネジメントを実践することで、どのような副次的な経営インパクトがあると考えますか？」という設問も行い、以下のような回答結果が得られました。**

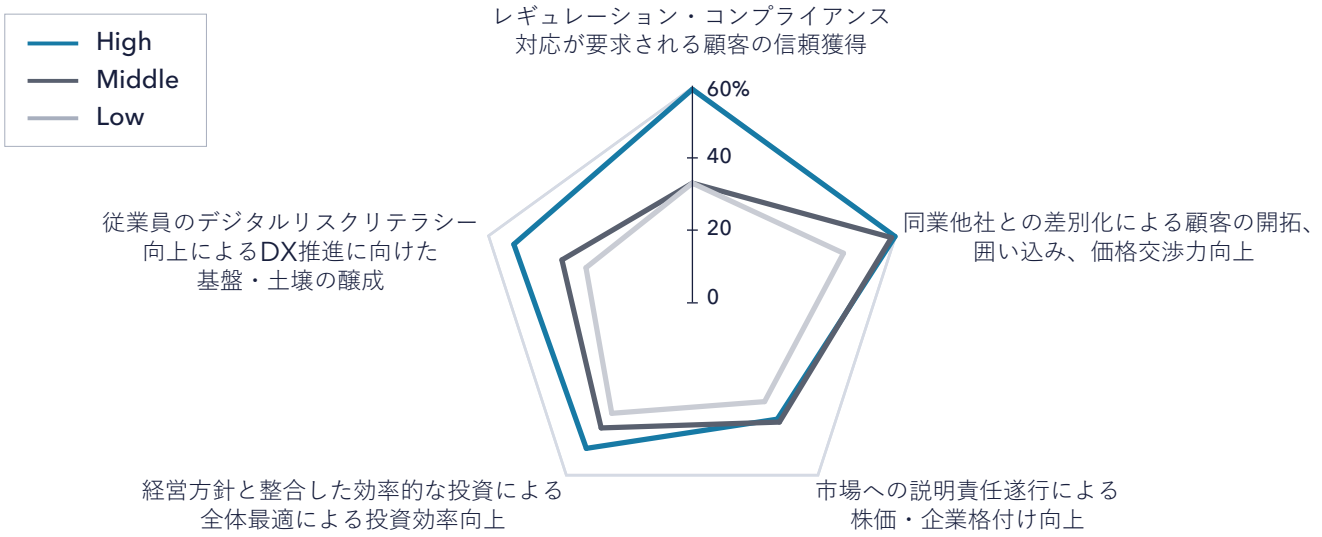
【図表11】副次的経営インパクトの認知



40%前後でリスクマネジメントが攻めの経営にもインパクトをもたらすと認知されていることがうかがえます。上位３つを挙げると「同業他社との差別化による顧客の開拓、囲い込み、価格交渉力向上」、「経営方針と整合した効果的投資による全体最適による投資効率向上」、「レギュレーション・コンプライアンス対応が要求される顧客の信頼獲得」となっており、DRM が競争力向上、信頼獲得にポジティブな効果をもたらすと認知されているようです。

また、成熟度別に見てみると、レギュレーション・コンプライアンス対応に関しては、High の企業と Middle/Low の企業で認知度に開きがあり、Middle と low においては DX におけるレギュレーション・コンプライアンス対応の重要性の理解はまだ進んでいないようです。
一部に温度差があるものの、全体的には DRM を後回しにすると、むしろ DX が停滞しかねないという理解は徐々に浸透してきていると推察されます。

【図表12】副次的経営インパクトの認知（マチュリティ別）



DXを成功に導くリスクマネジメントの構築

最後に DX を成功に導くリスクマネジメントについて解説します。
DRM の実装では、仕組みの構築だけでなく、経営層を理解・関与させることで、各種 DX プログラムの期待効果やスピードの確保を DRM の目的として設定することが肝要です。
DX を成功に導く DRM の要件としては右記の 5 項目が挙げられます。
デジタルリスクカタログは、DX 推進によりビジネスに影響を与えるリスク要因をリスクカタログとして整備したものです。これを整備しておくことで、DX プログラムごとに想定リスクを網羅的に洗い出すことが可能になります。
冒頭に記載したとおり、DX の特性の観点から大きく 4 つの分類でデジタルリスクカタログを整備することも 1 つの方法です。

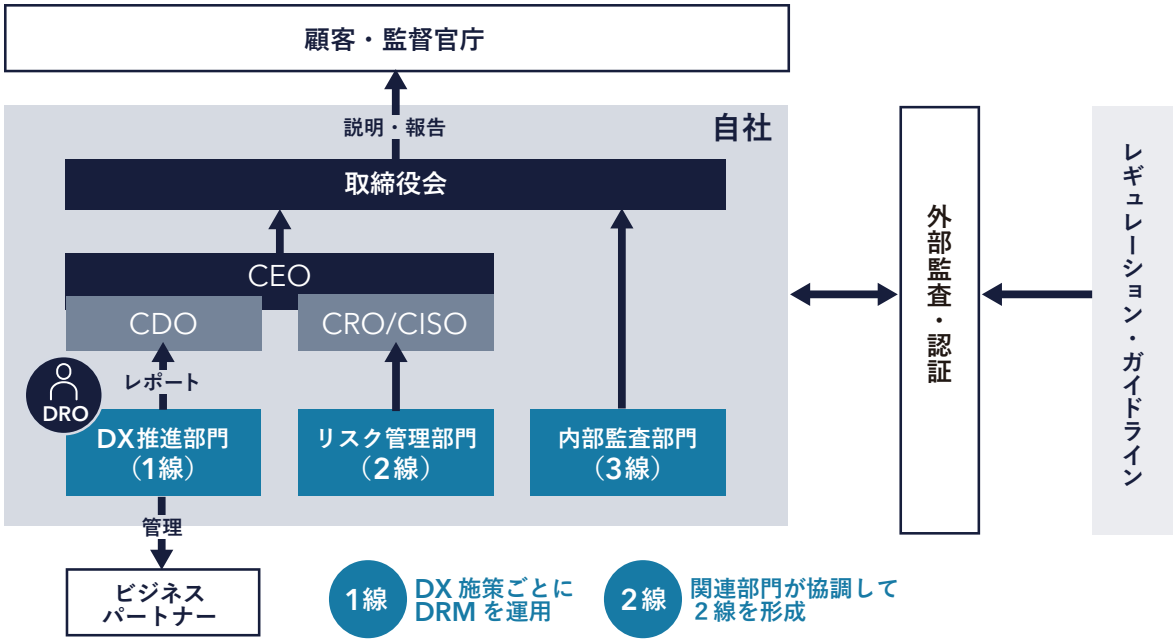
- **デジタルリスクカタログの整備**
- **DRMを有効に機能させるための3線ディフェンスを採り入れたガバナンス構築**
- **DXプログラムごとにDRMを運用するプロセスの整備**
- **DXプログラムごとに1線側にデジタルリスクオフィサー（DRO）を設置**
- **DROのレポートラインはCDO（チーフデジタルオフィサー）**

デジタルリスクカタログの例

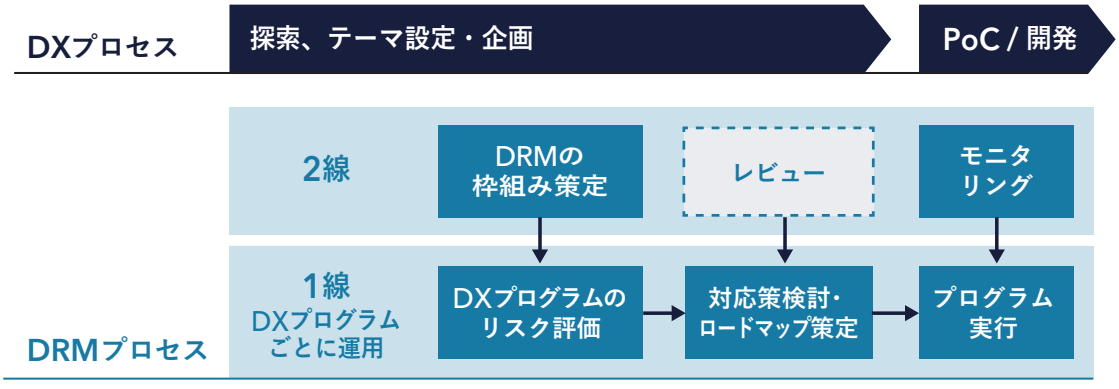
データ保護リスク	新技術適用リスク	ビジネスモデル変革リスク	プロセス変革リスク
• 重要データ保護 • プライバシーデータ保護	• クラウドリスク • APIセキュリティ • IoTセキュリティ • AIリスク	• コンプライアンスリスク • デジタルサプライチェーンリスク	• 不正・誤謬リスク • デジタルレイバーリスク • 生産性低下リスク • 事業継続リスク

デジタルリスクカタログをインプットに、各 DX プログラムに関与するデジタルリスクオフィサー（以下 DRO）が、施策のリスク評価、対応策の検討、ロードマップの策定、施策実行などを主導します。
その際、DRO が関与する 1 線（DX 推進部門）側の取り組みを、2 線（リスク管理部門）側がレビュー、モニタリングします。さらに内部監査部門が最終的な監査を行う 3 線としての役割を果たし、ガバナンスをより強固にするという体制です。

このようにリスクガバナンスとして 3 線ディフェンスを取り入れ、2 線でデジタルリスクカタログの整備を含む DRM の枠組み策定やモニタリングを（特にレギュレーション対応では必須）を行うことで、DX の信頼性を確保し、ステークホルダーへの説明責任を果たすことにもつながります。



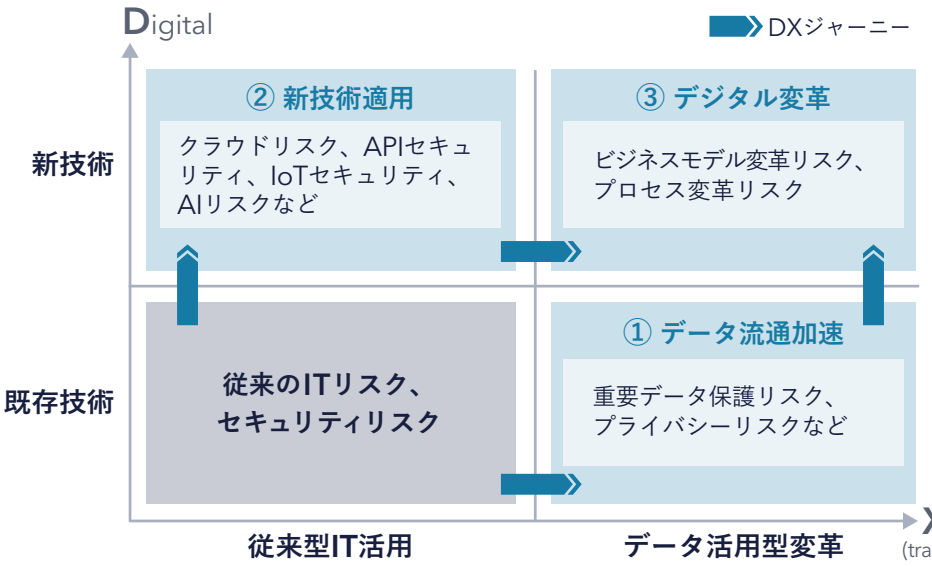
実際の DRM プロセスの運用では、DX プロセスの進捗に合わせて、1 線・2 線で役割分担して進めることになりますが、基本的には 1 線の DX 推進部門がリスクオーナーとして、2 線の支援を受けて DRM を実践することとなります。
ここで生じるのが二重、三重のリスクマネジメントによって、DX の推進にブレーキがかかるのではないかという懸念です。しかし、DX プログラムにおけるリスクとの向き合い方は、既存のビジネスとは異なります。未知の領域に挑むからこそ、評価の段階で一定のリスクテイクは必要なものと考え、ある程度許容しながら施策を進めるバランス感覚が必要となります。
そのためにも、リスクが顕在化した際に、速やかに検知して対応するビジネスレジリエンスが求められます。
また、2 線側では、幅広いリスクに対する知見を有し、2 線の他部門と協調しながら 1 線をサポートできる人材の確保も今後の課題です。



DXで注力すべきリスクマネジメントのテーマ

DXジャーニーを踏まえたリスク認識

DX プログラムのフェーズ（DX ジャーニー）の進展度合いよって、対応するリスクテーマも異なるため、自らの立ち位置、DX プログラムの特性を踏まえたリスク認識が必要となります。



① つながるリスク
パブリッククラウドなどを活用して企業内・企業間のデータ流通が加速し、データ保護リスクが高まります

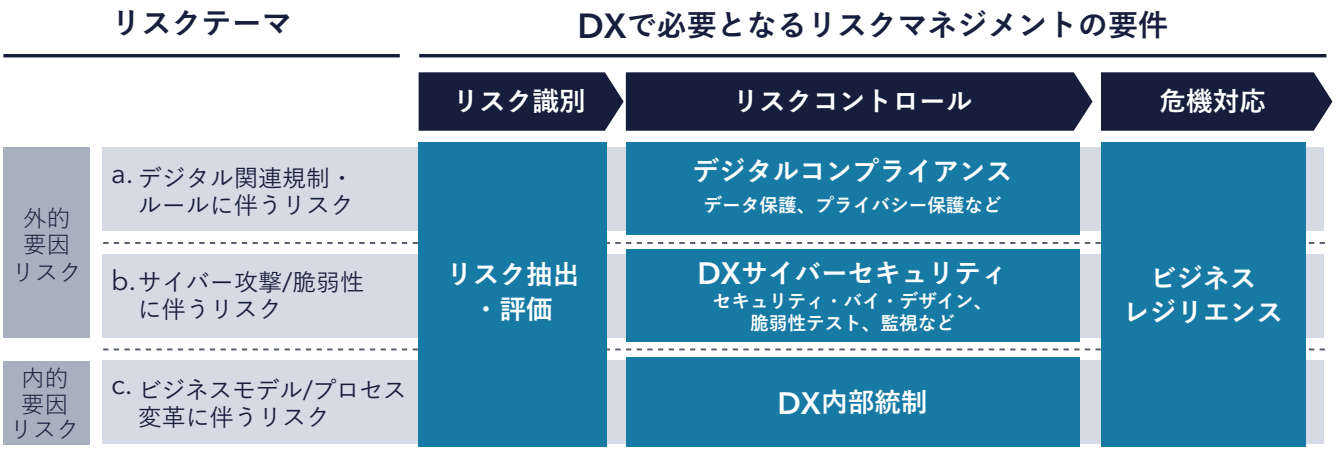
② 新技術適用リスク
AI や IoT、5G 導入により個別テクノロジーの脆弱性や未知の脅威に晒されます

③ デジタル変革リスク
本格的な DX の推進により、①と②の複合的なリスクに晒されます

DXで注力すべきリスクマネジメント

前述のように DX ジャーニーの進展度合いに応じたリスク認識、リスクテーマを捉えたうえで、リスク識別、リスクコントロール、危機対応の活動を組織として実装することが、DX 時代におけるリスク管理部門の役割です。
例えば、GDPR や NIST SP800-171 といったデジタル関連の規制やルール整備への対応としての“デジタルコンプライアンス”では、情報セキュリティ部門や法務部門、システム部門が協調することが求められますし、パブリッククラウドや API などを活用しながら外部システムと連携する場合には、“DX サイバーセキュリティ”としてパブリッククラウド上でシステム構築を行う際の脆弱性への対応から連携先のリスク評価まで、幅広いリスクへの対応を現業部門とセキュリティ部門、さらには内部監査部門などが協調しながら DX プログラムの信頼性を確保します。

また、デジタルレイバー導入による自動化などが進むと、手動とは異なる不正リスクや誤謬リスクなどへの対応が必要となるため、IT 全般統制をはじめとする“DX 内部統制”の見直しや高度化を現業部門、IT 部門、内部監査部門が協調して取り組みます。



Ridgelinez は、デジタルリスクガバナンスの体制づくりや、
デジタルコンプライアンス、サイバーセキュリティ対策、
ビジネスレジリエンスなど、企業のDRMを包括的に支援する
コンサルティングを提供しています。

このようなデジタルリスクマネジメントの取り組みは、
DX同様に未知の取り組み、チャレンジングな取り組みでも
あります。DXにブレーキをかけるものとしてではなく、
DXプログラムを加速させ、信頼性を担保する取り組みとして
社会に浸透させてまいります。

参考文献

1. BBCNEWS, “TSB: How it all went so wrong for the bank”,, 27 April 2018
   https://www.bbc.com/news/business-43923561
2. Guardian, “TSB lacked common sense in run-up to IT meltdown, says report”,19,November,2019
   https://www.theguardian.com/business/2019/nov/19/tsb-it-meltdown-report-computer-failure-accounts
3. INDEOENDENT,” TSB IT meltdown cost bank £330m and 80,000 customers”,1,February,2019
   https://www.independent.co.uk/news/business/news/tsb-it-failure-cost-compensation-customers-switch-current-account-a8757821.html
4. BUSINESS INSIDER, “A Troubled Project To Replace Oracle With SAP Software Could Cost A New York Gas Utility Nearly $1 Billion”,7,October,2014
   https://www.businessinsider.in/enterprise/a-troubled-project-to-replace-oracle-with-sap-software-could-cost-a-new-york-gas-utility-nearly-1-billion/articleshow/44552010.cms
5. COMPUTERWPRLD, “Cost of troubled SAP project will skyrocket to nearly $1 billion, audit says”,3,October,2014
   https://www.computerworld.com/article/2691661/cost-of-troubled-sap-project-will-skyrocket-to-nearly-1-billion-audit-says.html
6. TheRegister,” Wipro hands $75m to National Grid US after botched SAP upgrade”,8,August,2018
   https://www.theregister.com/2018/08/06/botched_sap_implementation_national_grid_wipro_settlement_75m/

免責事項

1. 本資料は一般的な情報提供のみを目的としており、専門のアドバイザーによるコンサルティングに代わるものとして使用することはできません。
2. 当社は、本資料の記載項目及び内容につき、正確性、完全性、信頼性その他一切の表明・保証をするものではありません。
3. 本資料の記載項目及び内容は、当社の自由裁量により、撤回、変更、追加がなされうるものであり、当社はこれに拘束されず、一切責任を負いません。

Contact

Ridgelinez Limited
Risk Management
〒100-6922 東京都千代田区丸の内 2-6-1
丸の内パークビルディング 22F
03-5962-9391
contact-rm@ridgelinez.com
www.ridgelinez.com