Risk in review
フロントラインからリスクを管理する

6th Annual Study
2017 年

pwc

目次

2017年 Risk in review：調査方法

PwCは、第6回目となる2017年版『Risk in review』のために、全世界を対象に調査を実施しました。今回の調査では最終的に80カ国以上の30業種にわたる1,581人の企業幹部から回答を得ました。

回答者は取締役、C-levelの経営幹部、およびその直属の部下です。肩書きで最も多かったのは、Chief Risk Officer（CRO）、Chief Audit Executive（CAE）／内部監査部門長またはその直属の部下、Chief Financial Officer（CFO）、監査委員会の委員長または委員、Chief Executive Officer（CEO）またはその他の取締役でした。C-levelの経営幹部の回答者の割合は2016年の調査と比べて急増し、CEOとCROの数はいずれも31％の大幅増となりました（注：企業における肩書きはCAE／内部監査部門長、CRO／リスク管理部門長といった呼称の違いを加味したうえで分類しています）。

調査結果をより現実に即したものにするために、PwC社内のリーダーとOxford Economicsによる洞察を加え、さまざまな業界の企業幹部との一対一のインタビューも行いました。

回答者の組織の本社・本部所在地を見ると、北米が全体の34％を占め、これに欧州（33%）、アジア太平洋（19%）、中南米（7％）、中東・アフリカ（7%）が順に続きます。

調査の目的上、回答者を大きく六つのセクターグループに分類しました。消費・製造・サービス（CIPS）は回答者の40%を占め、これに金融サービス（33%）、テクノロジー・情報・通信・エンターテインメント・メディア（11%）、ヘルスケア（8%）、政府・公的機関（4%）、教育・非営利団体（2%）、その他（2%）が順に続きます。

今年の調査にご協力いただいた全ての方に謝意を表します。

問題の核心

フロントラインのリーダーシップ、協同的アプローチによる成功

2008年の世界金融危機からほぼ10年がたったが、その後遺症により企業は守りのリスク管理姿勢を取らざるを得ず、困難な状況を乗り切ろうと奮闘する中でリスク管理の責任を事業部門（第1ディフェンスライン）から第2ディフェンスラインに下げたままとなっている。

一方で、企業は、今日の複雑なビジネスリスク環境がもたらす新たな課題に直面しており、潮流が再び変化していることを目の当たりにしている。今やリスクの説明責任を第1ディフェンスラインがしっかりと担いつつ、三つのディフェンスラインがリスク管理に協同的に取り組むアプローチが、組織のレジリエンスと成長力を強化するカギとなり得る。この協同的アプローチとは、第1ディフェンスラインが戦略と整合したリスク判断を的確に行い、先見的な第2ディフェンスラインが効果的な取り組みと時宜を得た協議や連携を通じて意思決定に影響を及ぼし、勤勉で独立した第3ディフェンスラインが組織の保護と価値の実現という自らの本来の使命に注力するというものだ。

調査データを前年のものと比較したところ、「事業部門と企業幹部は、主要なビジネスリスクのオーナーシップとリスクに関する意思決定のオーナーシップを一致させることにより、主導的な役割を果たしつつある」という明確なトレンドの存在が明らかになった。

全体では、回答者の3分の2近く（63%）が「より多くのリスク管理責任を第1ディフェンスラインに移管することで企業の機動性が増す」（つまり、リスク事象の予測と影響の低減をより効果的に行えるようになる）と指摘している。また、「今後3年間でこうしたリスク管理責任の移管をさらに進める計画だ」とする回答者は46％に上った。

だが、私たちが**フロントライナー**と呼ぶ一つの回答者グループは、そのはるか先を進んでいる。

フロントライナーに分類される企業は調査サンプルの約13%を占め、「リスク管理における意思決定は第1ディフェンスラインが責任を持って行う」と回答する傾向が他の回答者よりもかなり強い。こうした回答者は「第1ディフェンスラインは大半のリスク領域に効果的に対処していると確信している」と述べ、その確信の裏付けとして、実効的なリスク管理のための実証済みの手法、および正式に承認された第2と第3のディフェンスラインを挙げている。

こうしたフロントライナーの強さはさらなる強さに繋がっている。というのも、フロントライナーは回答者全体と比べて、「売上高と利益率が今後2年間で増加する」と予想する傾向が強い。さらにフロントライナーは他の企業に比べ、ビジネス上の障害が少なく、不利なリスク事象とそれに関連する障害からの回復が早い傾向がある。その理由は、フロントライナーは三つのディフェンスラインに、それぞれの担当領域に集中させ、各ディフェンスラインが危機の局面で機動力と集中力を高められるようにしているからだ。

回答者は「フロントラインによる意思決定が理想的」であることに同意している

「フロントラインがリスクに関する意思決定と部門間の連携を主導している」と答えた回答者（フロントライナー）は

13%

にとどまったが、

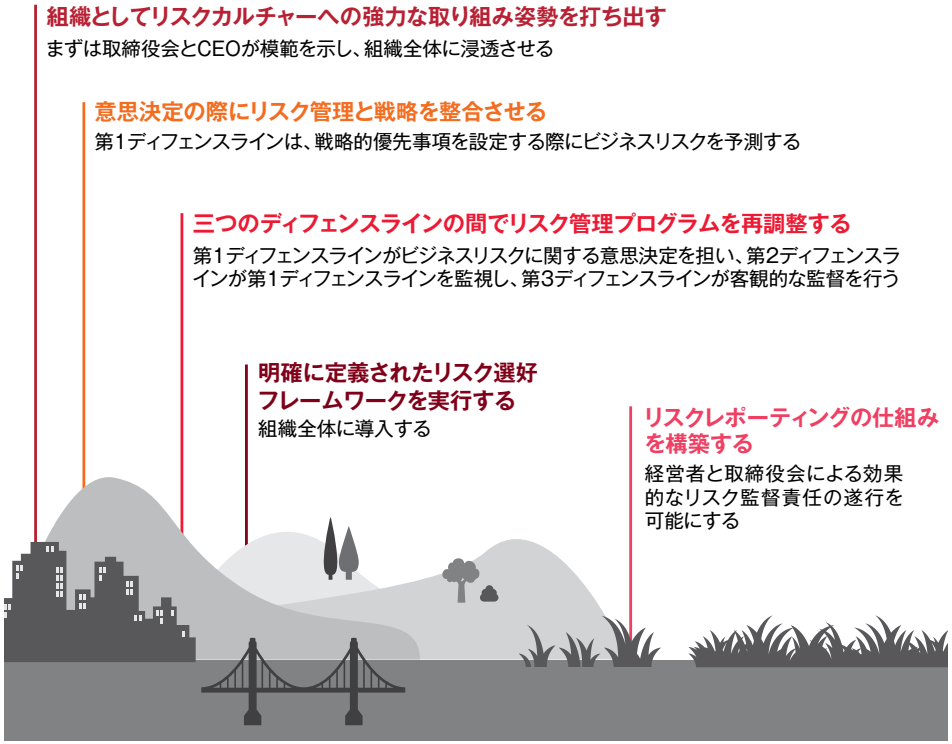
46%

は「リスク管理の責任をフロントラインに3年以内に移管する計画」であり、

63%

が「リスクに関する意思決定をフロントラインに移管することでリスクの予測と低減をより効果的に行えるようになる」ことに同意している

フロントラインが主導するリスク管理エコシステムでは、三つのディフェンスラインの間の連携が促され、説明責任が共有される。これにより、企業は現在のリスク環境が突き付ける課題に効果的に対処するための体制が整う。そうした状態に到達するために企業がすべきことは：



特定のリスク管理活動を第1ディフェンスラインに移管することは、リスク管理やコンプライアンスおよび監査機能への脅威ではなく、機会である。ビジネス主導のリスク管理とは、協同的で戦略的なフレームワークの中で全てのディフェンスラインが歩調を合わせることであり、これによって第2、第3のディフェンスラインは企業の価値創造プロセスにおける真のパートナーとなることができる。

フロントライナーとは誰か？

調査対象となった企業の13%がフロントライナーグループに分類された。調査結果からは、このグループは以下のような共通の強みを持つことが明らかになった。

1.「事業部門（第1ディフェンスライン）がリスクを効果的に管理するための適切な権限、人材、経営幹部レベルのサポートを有している」ことに関し、（強く）同意している

2.「特定のリスク管理責任を第1ディフェンスラインに移管することで企業はネガティブなリスク事象の予測と影響の低減策の実行をより効果的に行えるようになる」ことに関し、（強く）同意している

3. フロントラインは現在、今回調査した12領域のうち少なくとも6領域でリスクに関する意思決定を行っている

4. 他の回答者に比べ、明確で十分に理解されているリスク選好フレームワークを有し、主要なリスク管理に関する意思決定をそのフレームワークに従って行う傾向が強い

5. 1）リスク管理に適切な額の予算を充て、2）組織全体のリスクを集約するためにテクノロジーを活用し、3）日常業務にリスク管理を組み込んだ強力なリスクカルチャーを構築し、4）三つのディフェンスラインが強固な戦略的パートナーシップを示す、という傾向が強い

フロントライナーのCROは、自社では「リスク管理プログラムを成長の妨げではなく『成長を促進するきっかけ』と見なしており、独立したリスク管理機能とコンプライアンス機能が企業の事業部門に先見的かつ戦略的な指針を提供している」と述べる傾向が極めて強い。

消費・製造・サービス（CIPS）分野の企業は回答者全体の41%、フロントライナーグループの40%を占めている。一方、金融サービス分野の回答者は全体の29%、フロントライナーグループの33%を占め、相対的にフロントライナーに分類される割合が高い。

フロントライナーにおける金融サービス企業の割合は予想されていたとおりだが、CIPS分野の企業の割合は予想とは異なるかもしれない。だが、CIPS分野の企業がリスク管理の成熟度カーブを少しずつ押し上げていると考えられる理由がある。それは次のとおりである。

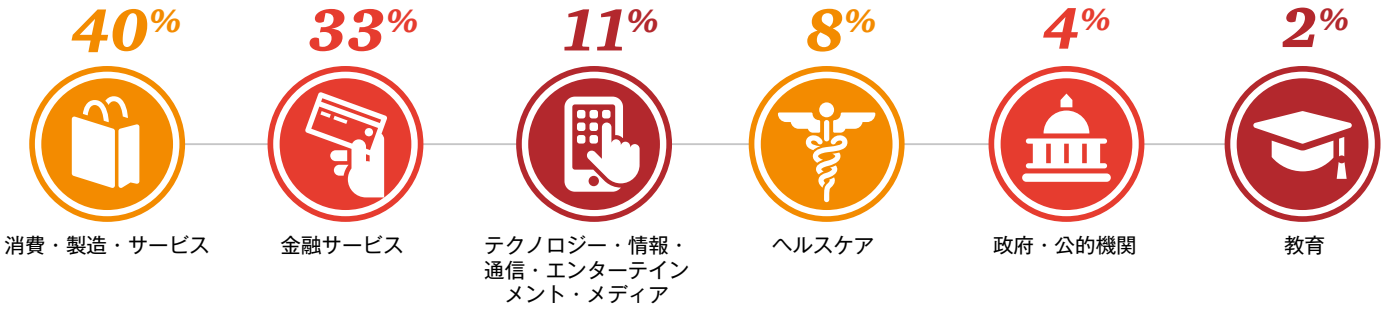
CIPS分野の企業は現在、より多くのリスク管理責任を第1ディフェンスラインに移管している

CIPS分野の企業では、第1ディフェンスラインがオペレーショナルリスクの管理を担う傾向が強い

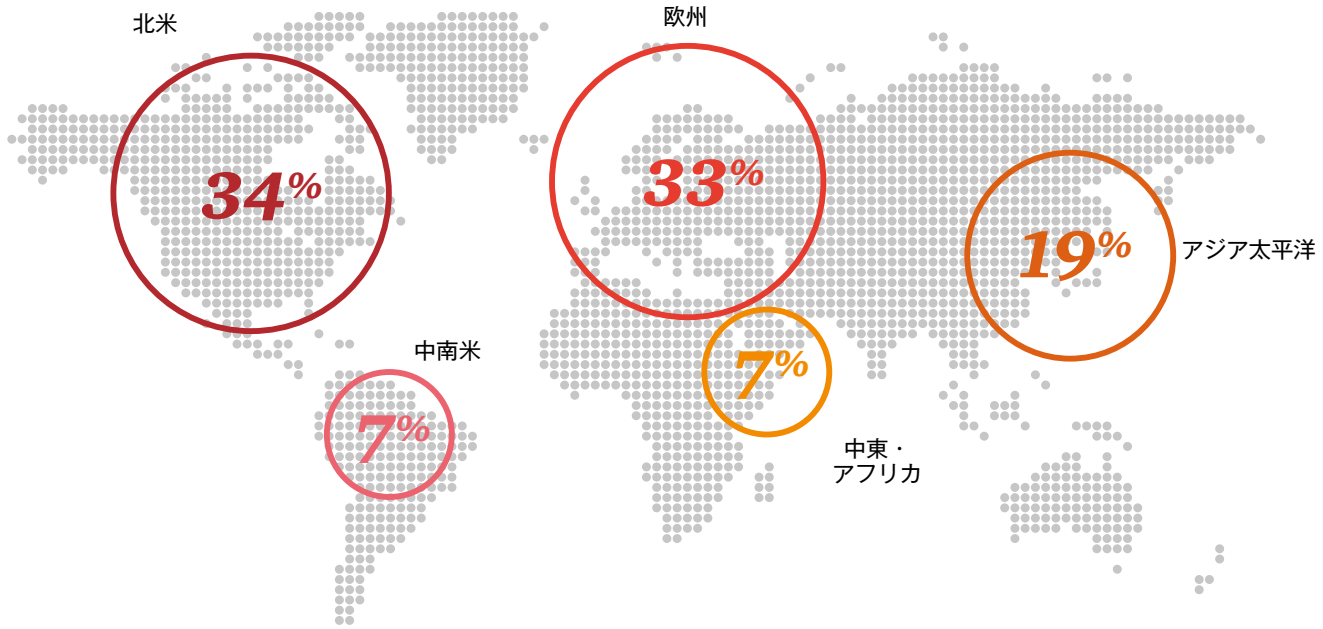
さらに、業務上の障害に直面したCIPS分野の企業の53%が障害に効果的に対処したと述べている（回答者全体では46%）

業界・地域別に見たフロントライナーの割合

業界別：



地域別：



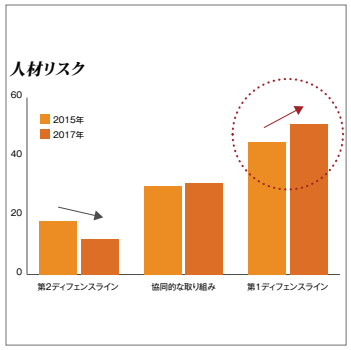
詳細分析

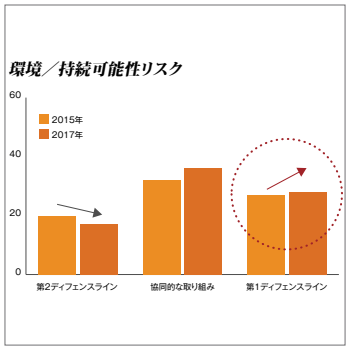
トレンド：有効性向上と成長に向けたビジネス主導のアプローチ

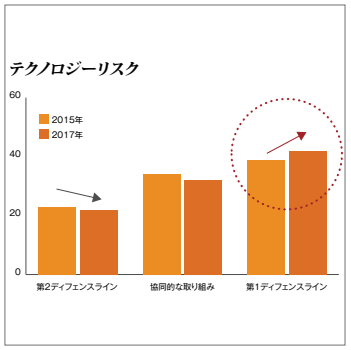
リスクに関する意思決定を第1ディフェンスラインが行っている企業では、リスク選好とリスク許容度に対してより厳格なアプローチが取られ、リスク管理全体の有効性が改善されており、その結果として売上高と利益率の伸びを予想する傾向が強いことが本調査で明らかになった。

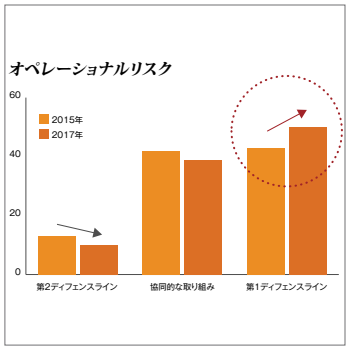
リスクに関する意思決定のオーナーシップを第1ディフェンスラインに移管するというトレンドは既に確固としたものになっており、回答者全員が「第1ディフェンスラインを構成する事業部門が単独または第2ディフェンスライン（リスクおよびコンプライアンス機能）と協同しながら、さまざまなリスクを管理している」と述べている。

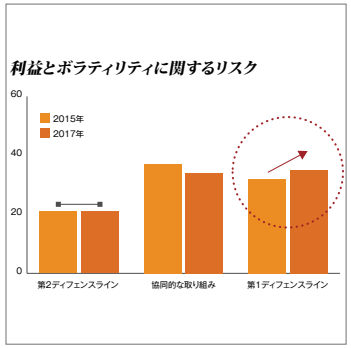
統計の推移は変化を示している。具体的には、『*Risk in review*』の2017年と2015年の調査結果を比較すると、「第2ディフェンスラインがリスクのオーナーとなって管理している」と回答した企業の割合は、両調査で対象となった11のリスク領域のうち8領域で横ばいか減少する傾向にあった。一方、「第1ディフェンスラインがリスクのオーナーとなって管理している」と回答した企業の割合は、11のリスク領域のうち5領域で増加した。

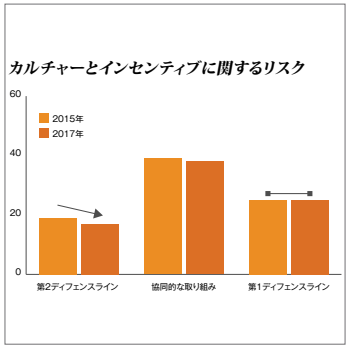


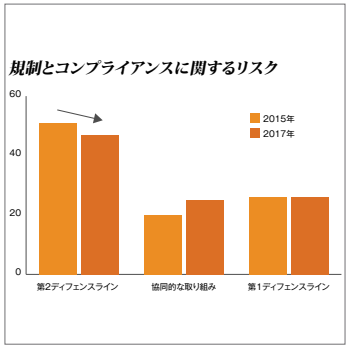


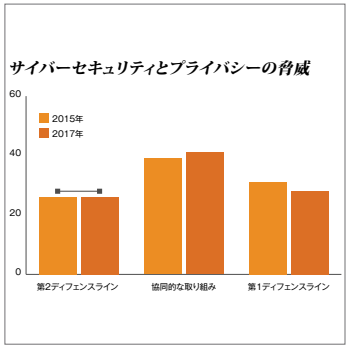


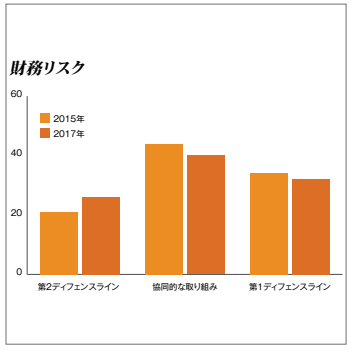


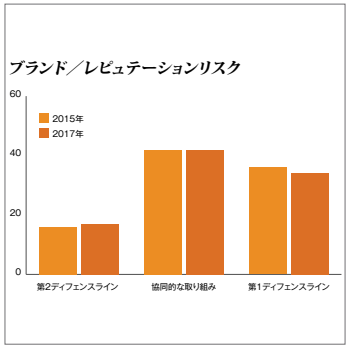


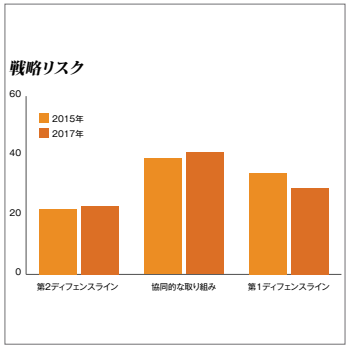












こうした変化は時代の流れに即している。多くの企業のリスク管理への主な取り組みは過去10年以上にわたり、サーベンス・オクスリー（SOX）法およびドッド・フランク法の要件に従ってコンプライアンス活動を行うことであった。こうした取り組みが、全社的なリスク管理のヒエラルキーにおけるChief Risk OfficerやChief Compliance Officerおよび監査リーダーの地位を引き上げたのはごく自然なことだが、SOX法の施行からほぼ15年がたち、2007年～2009年の金融危機からさらに遠ざかるにつれ、企業はリスクへの取り組みを足元の環境に応じたものに進化させようとしている。

PwCが直近で実施した第20回世界CEO意識調査では、回答を寄せたさまざまな業界のCEOが、企業が直面している最大の脅威として、経済成長の不透明感、行き過ぎた規制、重要なスキルの利用可能性、地政学的な不確実性、技術変化の速さを挙げた。加えて、サイバー攻撃の危険性、顧客の行動様式の変化、社会の不安定性が顕在化しており、第1ディフェンスラインがリスクオーナーとしてリスク管理の主導的な役割を果たさざるを得ない状況となっている。

SAP AGのChief Global Compliance OfficerであるMelissa Lea氏は、同社では直接的な繋がりが最も重要だと指摘したうえで、次のように述べている。「当社では第1ディフェンスラインの比重が高い。より多くのリスク管理の責任を現場に移管できるはずだ。リスク管理の責任の移管に際しては、リスク管理の責任をまずマネジメントが担当した後で従業員に任せるようにしている。これは、正しい判断を下すための適切な見通しを行うためだ。当社では、従業員が現場レベルや各国レベルで、あるいは特定のリスクがどのように顕在化するかを見通す優れた目線を持って、そうしたリスク低減アプローチを自ら実施するよう努めている」

効果的なリスク管理を実行するために必要なのは、組織全体の賛同を得ることだけではない。第1ディフェンスラインがリスク管理と戦略の整合性を担保し、さらに第2と第3のディフェンスラインが全社的なリスク管理のサポートに必要な人材を獲得できるようにすることも必要だ。フロントライナー企業からの調査結果は、より効果的なリスク管理と、売上高と利益率のより堅実な成長が、ビジネス主導型のアプローチによって支えられていることを示唆している。

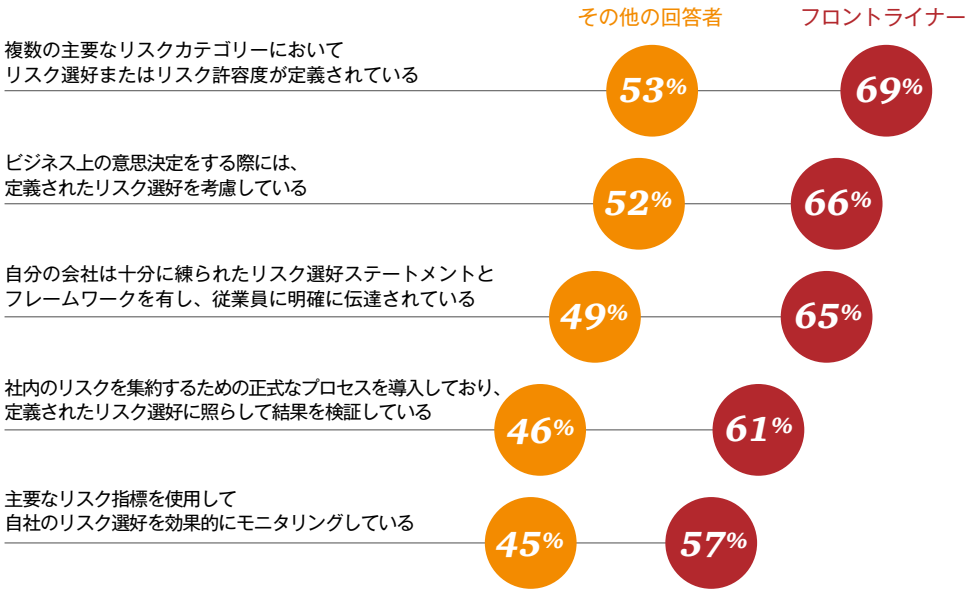
フロントライナーはどのように推進するのか?

フロントライナー企業は回答者全体に比べ、明確に定義されたリスク選好と先進的な実務を活用することにより、リスク管理に対して厳格なアプローチを取る傾向が強い。

フロントライナーはリスク管理における五つのベストプラクティスの実行状況に関して、他の回答者を最低でも12ポイント上回っている。

TIAAのSenior Executive Vice PresidentでChief Risk Officerを務めるSteve Gruppo氏は、「当社のリスクテイカーは第1ディフェンスラインだ。リスクに責任を負い、リスク選好を理解している。第2ディフェンスラインはそれを受けてビジネスパートナーに助言と課題を与え、ビジネスパートナーによる当社のリスクプログラムの導入を支援し、全社的リスクと事業部門の固有リスクがいずれもそのリスク選好に適合するように調整している」

フロントライナーはリスク管理に対してより厳格なアプローチを取っている

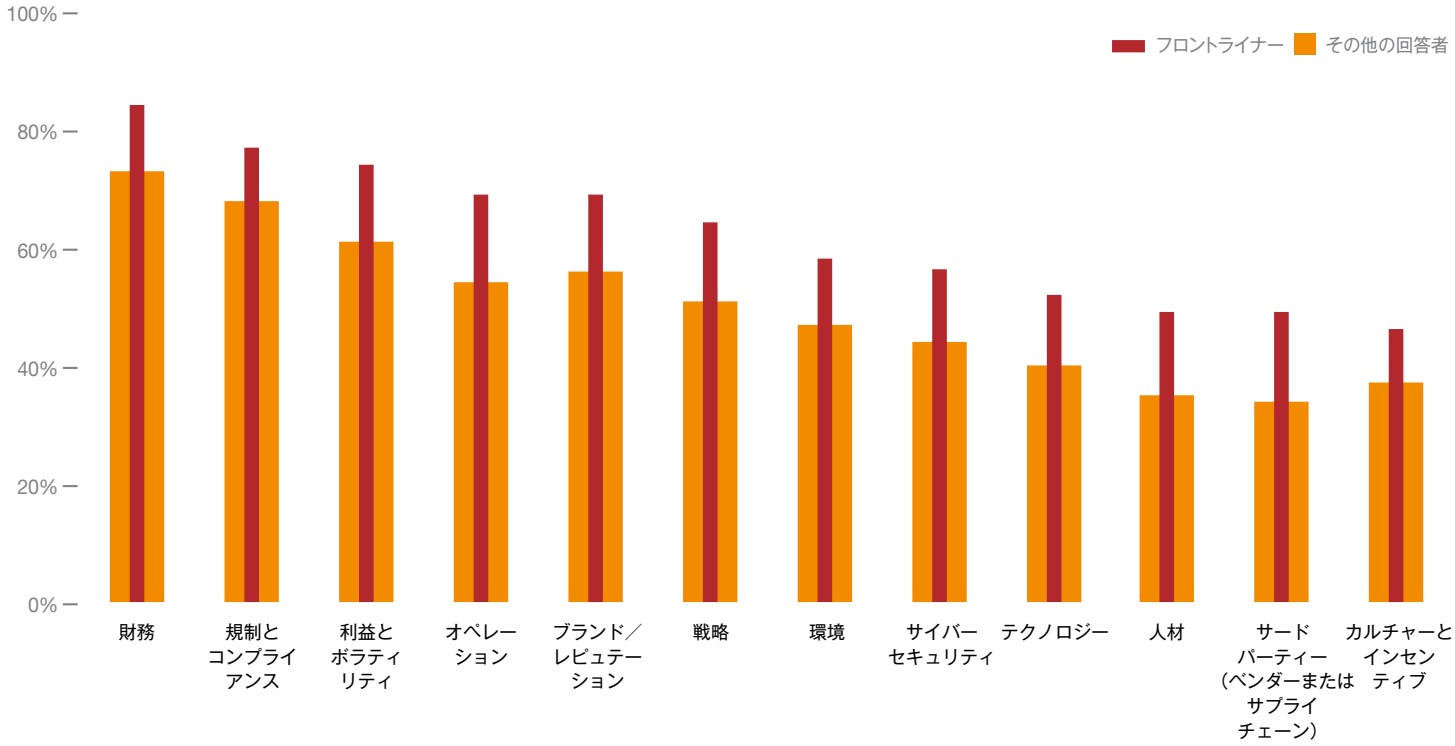


フロントライナーに分類される企業は、調査した全12領域で「リスクを効果的に管理している」と述べる傾向が他の回答者よりも強い。特に一部のリスク領域では違いが顕著である。

過去のリスク事象に関するフロントライナーの回答は、その自信が成功体験に基づいていることを示唆している。例えば、ネガティブなリスク事象に対処したことがあると回答した割合はフロントライナーの方が顕著に高かった。この傾向は、今回調査した「ビジネスに障害をもたらす12の要因」のいずれにも当てはまる。

ビジネスモデルや戦略の変化によって引き起こされた障害に直面した企業のうち、「実質的に回復した」と回答した割合がフロントライナーでは66%だったのに対し、それ以外の回答者ではこの割合が48%であった。オペレーショナルリスクによる障害に直面した企業では、「実質的に回復した」と回答した割合がフロントライナーでは63%だったのに対し、それ以外の回答者では46%であった。また、地政学的な混乱による障害に直面した企業では、「実質的に回復した」と回答した割合がフロントライナーでは56%だったのに対し、それ以外の回答者では39%であった。

フロントライナーはリスクをより効果的に管理している



フロントライナーのリーダーシップによる財務上のメリット

戦略と整合した効果的なリスク管理が財務パフォーマンスの改善を伴うことは過去のRisk in reviewの結果から明らかになっており、今年の調査結果が「第1ディフェンスラインによるリスク管理が財務指標の改善に繋がっている」と示唆していることに意外性はない。

第1ディフェンスラインが主導するリスク管理プログラムは、戦略、リスクオーナーシップ、および意思決定と歩調を合わせることにより、おのずと防御的・受動的ではなく戦略的・先見的なものとなる。ひいては売上高と利益率の力強い成長、市場シェアの拡大、従業員離職率の低下、障害に立ち向かう能力の向上に貢献する。

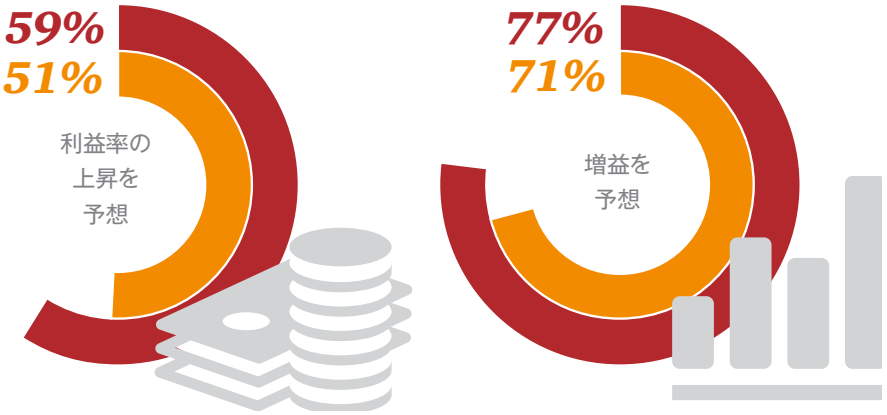
「リスクテイクをやめるつもりはない。目を見開いて、会社全体のリスク選好の枠内で、情報に基づく賢明なリスクテイクを行いたいと考えている。レーシングカーに例えるなら、ブレーキがあるからこそ加速する自信が得られる。直線コースで加速し、コーナーを曲がる時には車両を制御するためにブレーキを使う。つまり、ブレーキがない車に乗るよりもはるかに高い平均速度が得られる」

— *Nick Hirons氏, SVP for global ethics and compliance, GlaxoSmithKline*

結論：今後2年間の売上高と利益率の成長を予想する傾向はフロントライナーの方が他の回答者よりも強い。

フロントライナーは財務指標の改善を指摘している

今後2年間で：



組織に組み込まれた協同的リスク管理は全てのディフェンスラインにメリットをもたらす

第1ディフェンスラインがリスク管理において効果的なリーダーシップを発揮しても、第2ディフェンスラインのリスク管理機能やコンプライアンス機能の役割や影響が最小化されることにはならない。むしろ、第1ディフェンスラインによる効果的なリーダーシップは、リスクの認識と管理責任を企業カルチャー全体に浸透させ、最適な実効性を備えたリスクエコシステムを創出する取り組みによる必然の結果である。フロントライナーはリスク管理を戦略的かつ効果的に実行するため、単独でリスクを管理するのではなく、三つのディフェンスラインを結集した協同的なアプローチを推進している。

フロントライナーは、組織全体を包含する強力なリスクカルチャーの構築に注力している。こうしたリスクカルチャーは、C-Suite、取締役会、事業部門のリーダーシップが率先して模範を示すことによって醸成され、ビジネス戦略と整合したものとなり、リスクや障害へのより迅速かつ効果的な対応を可能にする。この種の組織は次のような体制を備える。

第1ディフェンスラインである意思決定者は、ビジネスリスクを予測し、戦略立案と戦術実行の両方にリスク管理を組み込み、さまざまなリスクが適材適所で管理されるように調整する。

第2ディフェンスラインであるリスク管理およびコンプライアンス機能は、第1ディフェンスラインと連携し、牽制機能を発揮してリスク管理プロセスを最適化する。

第3ディフェンスラインである内部監査部門は、統制を客観的にテストし、独立した立場から保証する。さらに第1と第2のディフェンスラインのリスク管理活動を評価する。

米国のある主要企業の内部監査部門長兼Chief Risk Officerは次のように指摘している。「物事を円滑に進め、うまく連携できるかどうかが問題だ。私は全社的リスク管理とリスク受容に関連する問題の意思決定者ではなく、調整役および連絡役であり、私の部下は事業部門と連携を図っている。懸念点を見つけてそれを検証するのは私たちだが、私たちの報告を聞いて最終的にリスクを受容するかどうかを決めるのはCEOおよび幹部が参加するリスク管理委員会だ。始めの2回、3回、4回の委員会で必ずしも合意が得られるわけではないが、最終的な論点は、『組織と株主にとって最善の選択は何か、それが私たちの目的と目標にどのように影響を及ぼすか』である」

強力なリスクカルチャーの重要性

成熟したリスクカルチャーでは、リスクの集約・記録・予測のためのリスクの分類に関して共通の理解があり、最適な情報収集のためにデータ分析などのテクノロジーが駆使されている。三つのディフェンスラインによる効果的なコミュニケーションを通じて組織のリスク選好とリスク許容度への基本的理解が広く浸透し、それを継続的なモニタリングとリスク関連の業績インセンティブ制度が後押ししている。

TIAAのSteve Gruppo氏は次のように述べている。「当社には、リスク選好を策定し、伝達するための構造化されたプロセスがある。このプロセスには取締役会が関与し、リスク選好ステートメントは取締役会によって承認される。リスク選好の策定と伝達は全社レベルと三つの主要事業部門のそれぞれで行われる。このプロセスには、リスクに対する姿勢に焦点を当てた定性的なステートメントと一連の定量的指標が高いレベルで組み込まれている」

全組織的な強力なリスクカルチャーを定義する指標を見ても、フロントライナーが他の企業の先を進んでいることが分かる。具体的には、

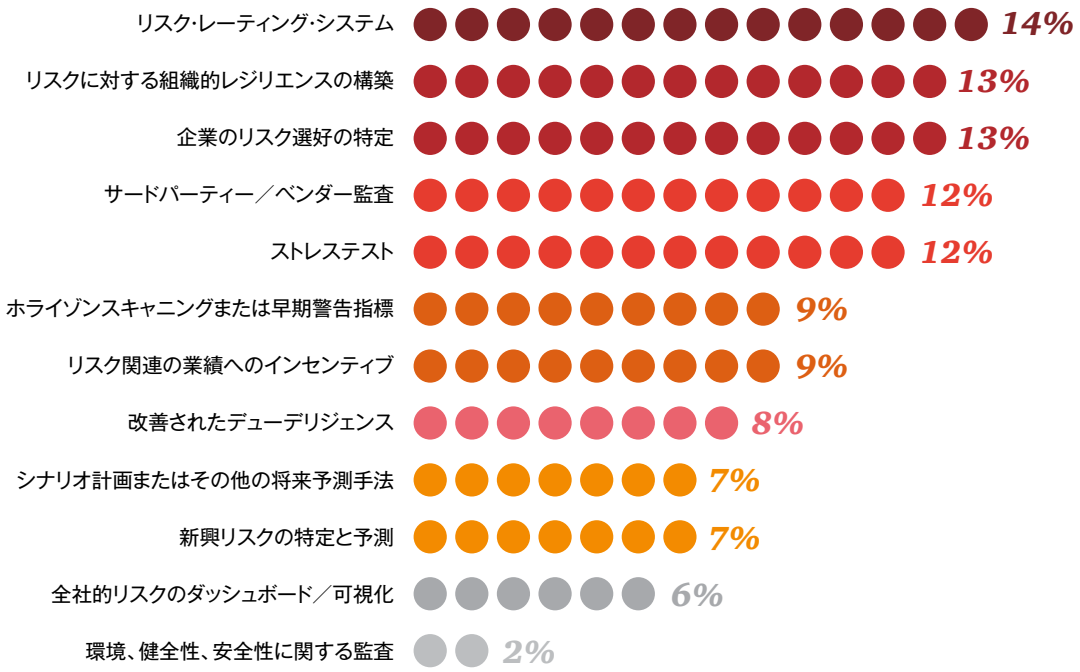
- ネガティブなリスク事象の発生後、外部のステークホルダーとコミュニケーションを積極的に取っている（49%対37%）
- 倫理およびコンプライアンスに関する研修を全従業員に義務付けている（80%対71%）
- リスク管理へのトップダウンとボトムアップのアプローチを実践するため、取締役会レベルのリスク委員会を一つまたは複数設置している（64%対54%）

- 第2ディフェンスラインが効果的に異議を唱え、第1ディフェンスラインに働きかけることができるカルチャーが奨励されている（55%対45%）

健全なリスクカルチャーを維持するには、リスク管理のための先進的なツールや手法を導入して使用することも重要だ。それを表す評価指標に関しても、フロントライナーは他の回答者を大幅に上回っている。

フロントライナーはリスク管理のためにツールや手法を使用する傾向が強い

フロントライナーが使用する傾向の強いツールと手法（「使用している」と回答した割合の他の回答者との差が大きいもの）



「私たちは、ビジネスとの普段のやりとりを含め、全ての業務を継続的なリスク評価プロセスとして見ている。私たちが別々に膨大なプロセスを実行しなければならないとすれば、ビジネスに十分に寄り添っていないことになる」

—Doug Watt氏, Senior Vice President and Chief Audit Executive, Fannie Mae

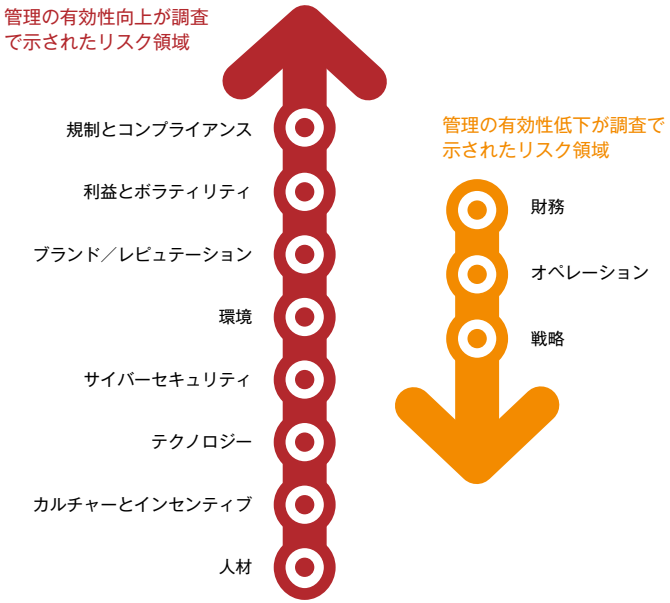
リスク管理が改善している組織とそうでない組織

2015年と2017年の調査結果の比較により、全体的なトレンドとして、大半のビジネスリスクについて管理の有効性が改善し、戦略的なリスク管理実務の利用が拡大していることが判明した。ただし、特定のリスク領域については管理の有効性がやや低下、または横ばいとなっている。

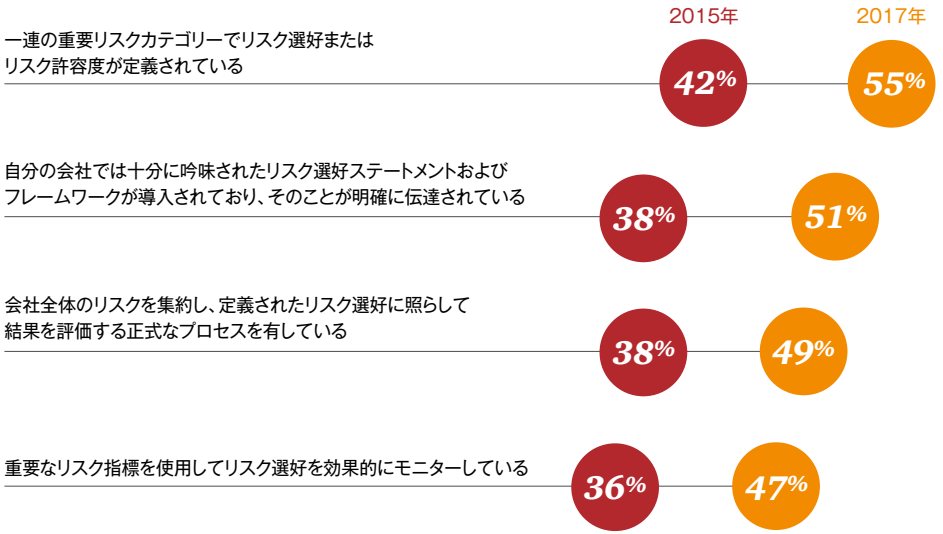
調査結果は、リスク管理が環境リスクとサイバーセキュリティリスクの領域で最も改善していることを示している一方、財務リスク、オペレーショナルリスク、戦略リスクへの対処については有効性がやや低下していることを示している。

過去2年間のデータから、リスク選好とリスク許容に対して特定のアプローチの使用が増えていることが確認された。これは、リスク管理が第1ディフェンスラインに戦略的に移管されていることを裏付けている。

2017年は2015年に比べてリスク管理の有効性が向上した



リスク選好へのアプローチの改善

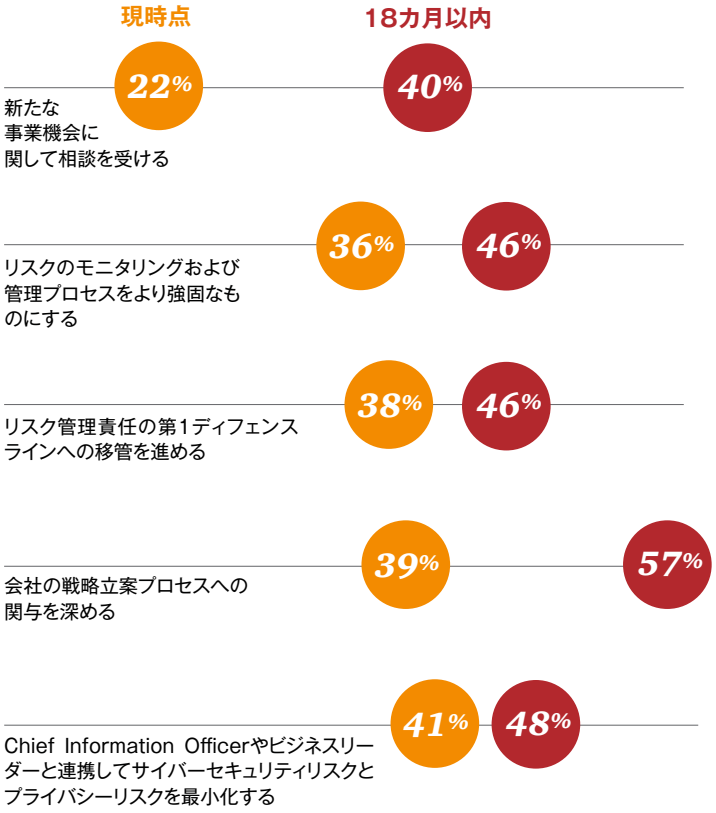


CROはより戦略的な役割を目指している

企業がリスク管理の意思決定を企業のリーダーシップと事業部門に移管している中で、Chief Risk Officer（CRO）も自らの役割と機能をより戦略的なものにしたいと考えている。現時点での優先課題として、戦略の立案への関与を深めたいと回答したCROは39%にすぎないが、今後18カ月の優先課題として同じことを尋ねると、この割合は57%に跳ね上がる。

第1ディフェンスラインがリスク管理の意思決定を行うエコシステムの中では、リスク管理機能およびコンプライアンス機能は、戦略、オペレーションおよび財務の観点から広範な業務、プロセスを理解したうえで、全体像を捉えなければならない。リスク管理機能およびコンプライアンス機能はそうすることにより、リスクに焦点を当てるカルチャーの中で重要なパートナーとしての価値を高めることができる。

リスク管理の有効性改善に関するCROの回答



また、2016年の調査結果と比較すると、「シニアリーダーは強固なリスク管理が持つ価値を理解している」と回答したCROの割合が大幅に増え（58%に対して72%）、「第2ディフェンスラインは成長のための触媒と見られている」と回答したCROの割合も増えた（36%に対して43%）。

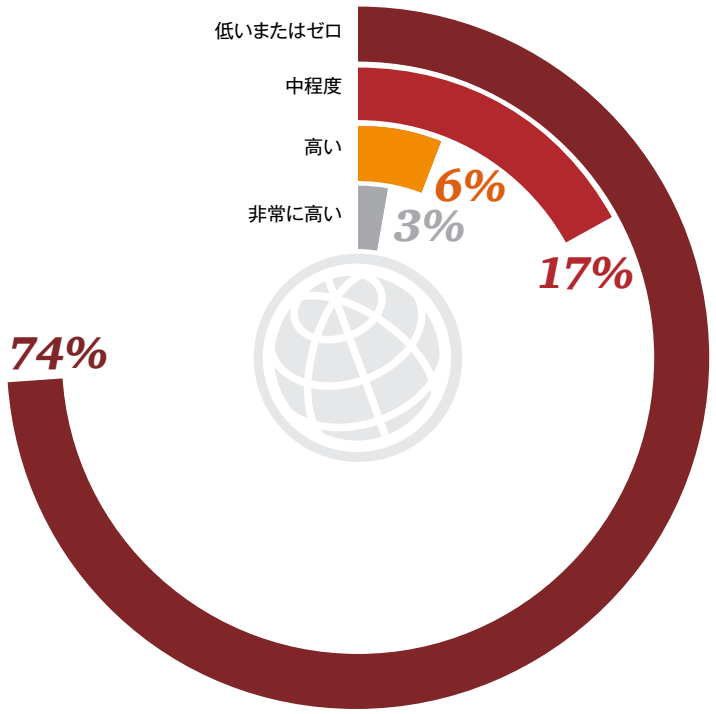
サイバーリスク管理の成熟度

かつてなく巧妙な手口を身に着けたサイバー犯罪者にとってデジタルプラットフォームが格好の犯罪の舞台となる中、サイバーリスクへの認識は本格化している。PwCが最近実施した第20回世界CEO意識調査では、世界のCEOの半数以上（53%）が「今後5年以内に、サイバーセキュリティとデータプライバシーの侵害が業界に対するステークホルダーの信頼を脅かすようになる」と予想していることが分かった。米国では、CEOの回答者の85%が、サイバー犯罪が組織の将来の成長の脅威となることをある程度または非常に懸念していると述べている。

サイバー犯罪とデータプライバシーのリスクは、今や企業の業務のあらゆる側面に影響を及ぼす可能性があり、業界がモノのインターネット（IoT）をはじめとする新しいテクノロジーとの接点を広げる中で、その脅威は増す一方だ。私たちは、サイバーリスク管理に秀でた組織について学び、回答者が新たなサイバーセキュリティの現実にどのような対応体制を取っているか整理するため、サイバーリスク管理の成熟度モデルを作成した。全てのサンプルの中で最も成熟度の高い回答者は次の四つの実務を全て導入している。

1. Chief Risk Officer（CRO）とChief Information Officer（CIO）／Chief Technology Officer（CTO）はサイバーセキュリティとプライバシーリスクの監視に共同で責任を負っている。
2. サイバーセキュリティとプライバシーリスクはCIO／CTOが管理している。
3. CIO／CTOは各事業部門および各機能と協力してデータを保護している。
4. 機能横断的なサイバーセキュリティ／情報リスク委員会を設置している。

サイバーリスク管理の成熟度（全回答者）



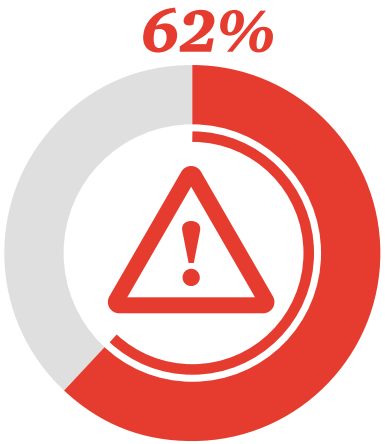
調査では、全てのセクターで全ての回答者が「今後数年以内にサイバーリスクが企業に極めて大きな破壊的影響をもたらす」と予想している。こうした見方が新たな前提となる中で、高度に進化したサイバーリスク管理の実務を備えた企業は明確な競争優位性を得ることになる。

サイバーリスクは今後3年間で大きく高まると予想されているにもかかわらず、サイバーリスク管理の成熟度が高い企業はほとんどない。

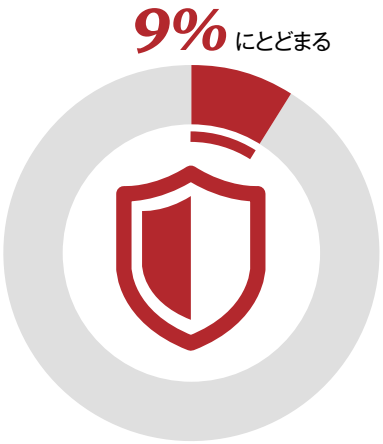
1,581人の回答者のうち「サイバーリスク管理の成熟度は非常に高い」と述べた回答者の割合は3%にとどまり、「高い」と回答した割合は6%、「中程度」と回答した割合は17%であった。注目されるのは、回答者の3分の2(66%)が四つの成熟度基準の一つだけを満たす「成熟度の低いグループ」に分類され、8%が「成熟度ゼロ」に分類された。ただし、サイバーセキュリティは過去の調査結果と比較してリスク対応の有効性に最も改善が見られたリスク領域の一つである。このことから判断すると、企業が自らの管理能力への自信を深めているにもかかわらず、サイバーリスクに対する姿勢は全く防御的なものにとどまっており、サイバーセキュリティや市場に対する競争優位性の強化に役立つ先進的な実務はまだ採用されていないと考えられる。

多くの企業は「最も肥大化しているリスクはサイバーリスクとプライバシーリスクである」と見ているものの、備えができている企業はほとんどない

「今後3年でサイバーリスクが破壊的影響をもたらす」と予想している回答者は



だが、サイバーリスク管理の成熟度が「非常に高い」または「高い」と答えた回答者は



「サイバーリスクやアンチマネーロンダリングに地域単位でこれ以上対処することは実質的に不可能になっている。ネットワークを通じて世界と繋がり、世界規模のシステムを稼働させるのであれば、適用している統制レベルを全ての共有化される環境で同じ水準に設定する必要がある。そうしなければ、企業のセキュリティ強度は最も脆弱な場所と同じレベルでしかない」

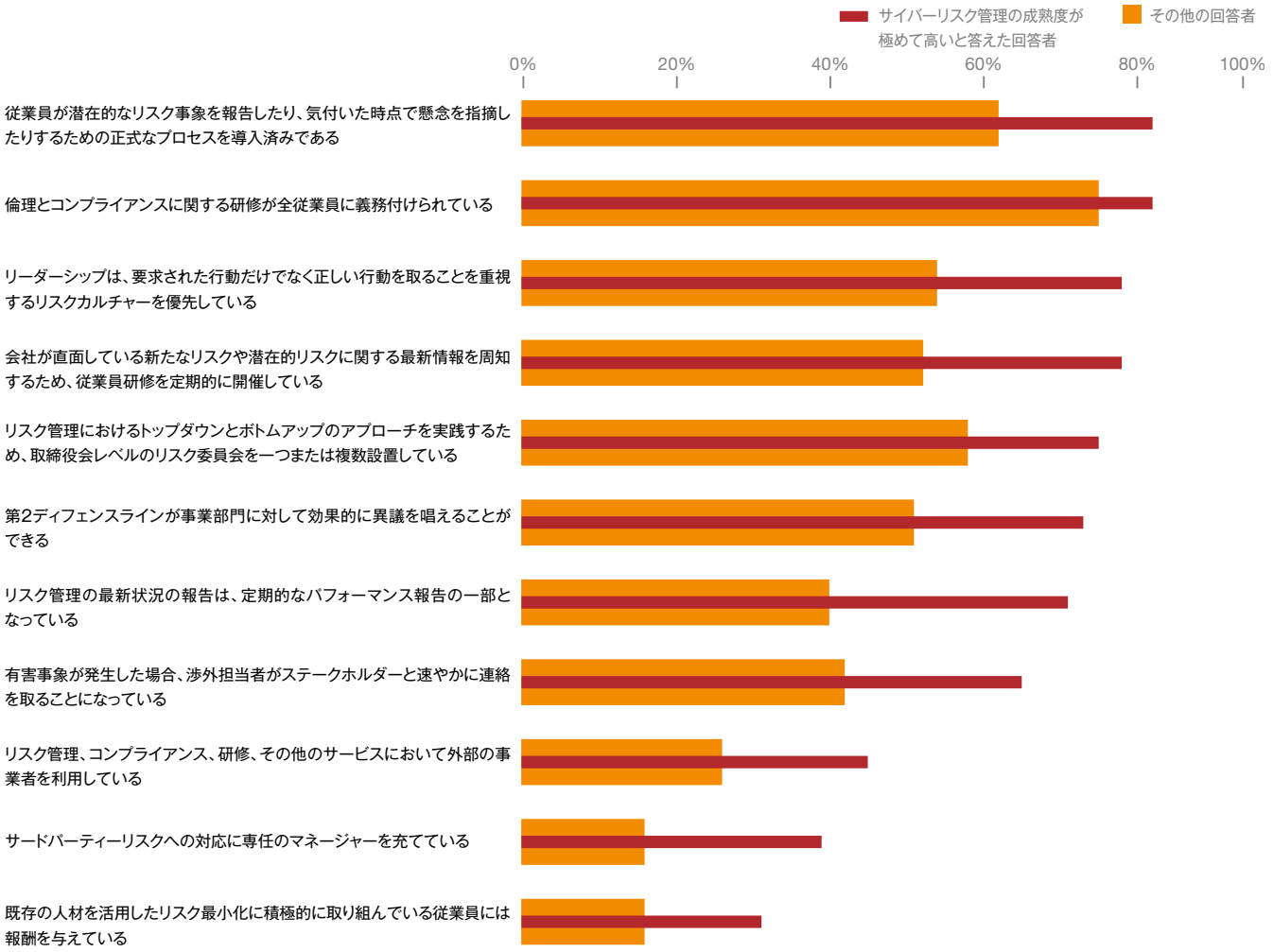
—Lisa Humbert氏, Managing Director, Chief Information Risk Officer, and Head of Information Risk Management, MUFG Union Bank, N.A.

企業のサイバーリスク管理の成熟度の改善には見た目以上のメリットがあるようだ。

私たちの分析では、こうした成熟度が他の領域における高度なリスク管理能力の指標となっている。例えばサイバーリスク管理の成熟度が高い企業は、戦略、オペレーション、ブランド、規制、財務などの重要リスクの管理能力も高く、リスクカルチャーのあらゆる指標が回答者全体の平均を大きく上回っている。

次の例は、フロントライナーの成長率見通しの高さを反映している。まず、サイバーリスク管理の成熟度を示す四つの実務を全て導入していると答えた回答者の63%が「今後2年間で利益率が上昇する」と予想している（その他の回答者では50%）。さらに、成熟度カーブで最も高いスコアを記録した企業では、増収を予想する傾向もやや強い（75%対71%）。

サイバーリスク管理の成熟度が高い企業はリスクカルチャーも優れている



MUFGケーススタディ：グローバルな成長が規制要件の増大をもたらす

三菱UFJフィナンシャル・グループ（MUFG）は2014年、三菱東京UFJ銀行（BTMU）の米国における支店銀行業務とUnion Bank, N.A.を統合し、MUFG Union Bank, N.A.という新たな名称の下で、統合された米国銀行事業の業務を開始した。統合された事業は法人および投資銀行の顧客、商業銀行、富裕層と個人の顧客にサービスを提供しており、世界で最も信頼される金融グループになるというMUFGのグローバルビジョンに忠実であり続けながら、米国における野心的な成長戦略を追求している。

MUFG Union Bank, N.A.は他の世界的な大手金融サービス企業と同様、厳格化される規制要件を順守しなければならない。MUFG Union Bank, N.A.のManaging DirectorでChief Information Risk OfficerとHead of Information Risk Management（IRM）を兼務するLisa Humbert氏は次のように述べている。「当社は事業を統合する前は大手金融機関に分類されていなかったが、今では大手金融機関に分類され、規制当局からより厳しい監視と検査を受けるようになった。例えば、米連邦準備理事会（FRB）の健全性強化基準（Enhanced Prudential Standards）、米通貨監督庁（OCC）の高度化された基準（Heightened Standards）、強化されたサイバー規制などだ」

こうした要件に対応するには、さまざまなレベルの変革を全社で推進することが必要になる。銀行は、規模と複雑さが増すに従って、リスク管理戦略とアプローチを進化させなければならない。このプロセスでは、ガバナンスの強化、重要な情報リスクを定義したリスト、脅威、統制、手続き、指標、報告を包含した正式な情報リスク管理（IRM）フレームワークを確立することになる。金融サービス企業の場合はさらに、役割と責任が明確化され、明解な構成要素とその機能に関する説明がなされ、一貫性のある分類方法とリスク評価手法を備えた強固なIRM管理基盤を確立しなければならない。IRM組織は、銀行がさまざまな種類のリスクと脅威を一貫した形で管理できるようにするため、全社的リスクガバナンス機能とオペレーショナルリスク管理機能と連携する。

Humbert氏は「私たちは、高度化された規制要件を満たし、一部のリスク領域については他のリスク領域よりも早期に対処するため、すぐに行動を起こす必要があった」と述べている。

MUFGのような世界的な金融サービス企業にとって、三つのディフェンスラインで構成されるリスク管理モデルの採用は不可欠だ。このモデルでは、効果的で先見的かつ持続可能なリスク管理を可能にするため、それぞれのディフェンスラインがリスク管理における自らの役割を理解したうえで他のラインと連携する。事業部門（第1ディフェンスライン）はそれぞれの事業領域におけるリスクの管理に責任を持ち、意思決定プロセスの一環としてリスク要因を評価しなければならない。IRMを含むリスク管理部門とコンプライアンス部門（第2ディフェンスライン）は全社のフレームワークを定義し、第1ディフェンスラインがそのフレームワークを順守しているかどうかを評価して問題点を指摘する。内部監査部門（第3ディフェンスライン）は、プロセスと統制が順守され、適切なリスク管理フレームワークが構築されていることを独立した立場から保証する。

「第1ディフェンスラインを担当する事業部門にとっては、自らの意思決定または導入したテクノロジーが情報リスクにどのような影響を及ぼすかを理解することが重要だ。情報リスクは最終的に、それぞれの事業部門に直接的な影響を及ぼすからだ。MUFGのリスク管理について協議する時には、全員が協力して取り組むことが明確に意識されている」

Humbert氏はさらにこう述べている。「例えばIT担当者の場合、『重要なIT環境に脆弱性が存在し、技術では解決できない場合、そのリスクはIT部門に影響を及ぼすことになるのか』という問いかけをしなければならない。犯罪者が脆弱性につけ込んだ場合、ビジネスだけでなく会社のレピュテーションなど広範囲に影響が及ぶ可能性があるが、リスクにさらされるのはビジネスである。当社は三つのディフェンスラインで構成される効果的なリスク管理モデルを採用することで、こうした問題を把握し、直面するリスクに共同で素早く対処するための洞察力とツールを備えるようになった。リスクカルチャーと意識改革の研修も、シニアリーダーからITチーム、組織の構成員をはじめ、情報リスクの管理に何らかの形で関与している全てのレベルで必要だ」

リスクカルチャーの成熟度

リスクカルチャーの成熟度を評価するため、成熟したリスクカルチャーの特徴である11の実務について質問し、所属する組織がそれぞれの実務を実践していると答えた回答者には、カルチャーの成熟度を評価するための指標として1ポイントを付与した。成熟度が低い回答者のスコアは0ポイント～2ポイント、成熟度が中程度の回答者のスコアは3ポイント～5ポイント、成熟度が高い回答者のスコアは6ポイント～8ポイント、成熟度が非常に高い回答者のスコアは9ポイント～11ポイントである。金融サービスとヘルスケア関連の組織は全体的に高いスコアを示した。

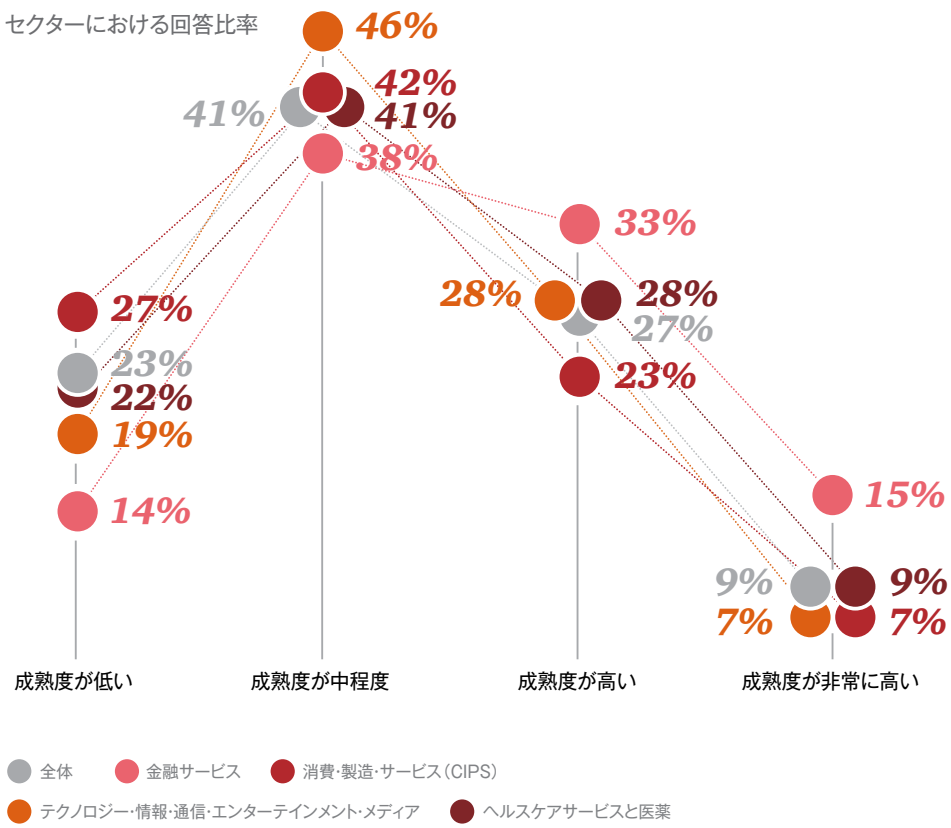
大半のセクターの回答者が「倫理とコンプライアンスに関する研修が義務付けられている」としているが、この質問に「はい」と答えた人の割合が最も高かったのは金融サービス（81％）とヘルスケア（79％）であった。多くのセクターで導入されているその他の実務には、「従業員が懸念を指摘したり潜在的なリスク事象を報告したりするための正式なプロセスを導入している」（最も多かったのは金融サービスの70％、次いでヘルスケアの66％）と「取締役会レベルのリスク委員会を一つまたは複数設置している」（最も多かったのは金融サービスの72％、次いでヘルスケアの56％）がある。

全てのセクターで全般的に導入が遅れている実務の一つは、「既存の人材を活用したリスクの最小化に積極的に取り組んでいる従業員に見返りを与えている」であり、これに「はい」と回答した人の割合が20%を超えたセクターは一つ（ヘルスケア）しかなかった。同様に、「サードパーティーリスクへの対応に専任のマネージャーを充てている」についても、「そうしている」と回答した人の割合が20%を超えたのは金融サービスだけであった。

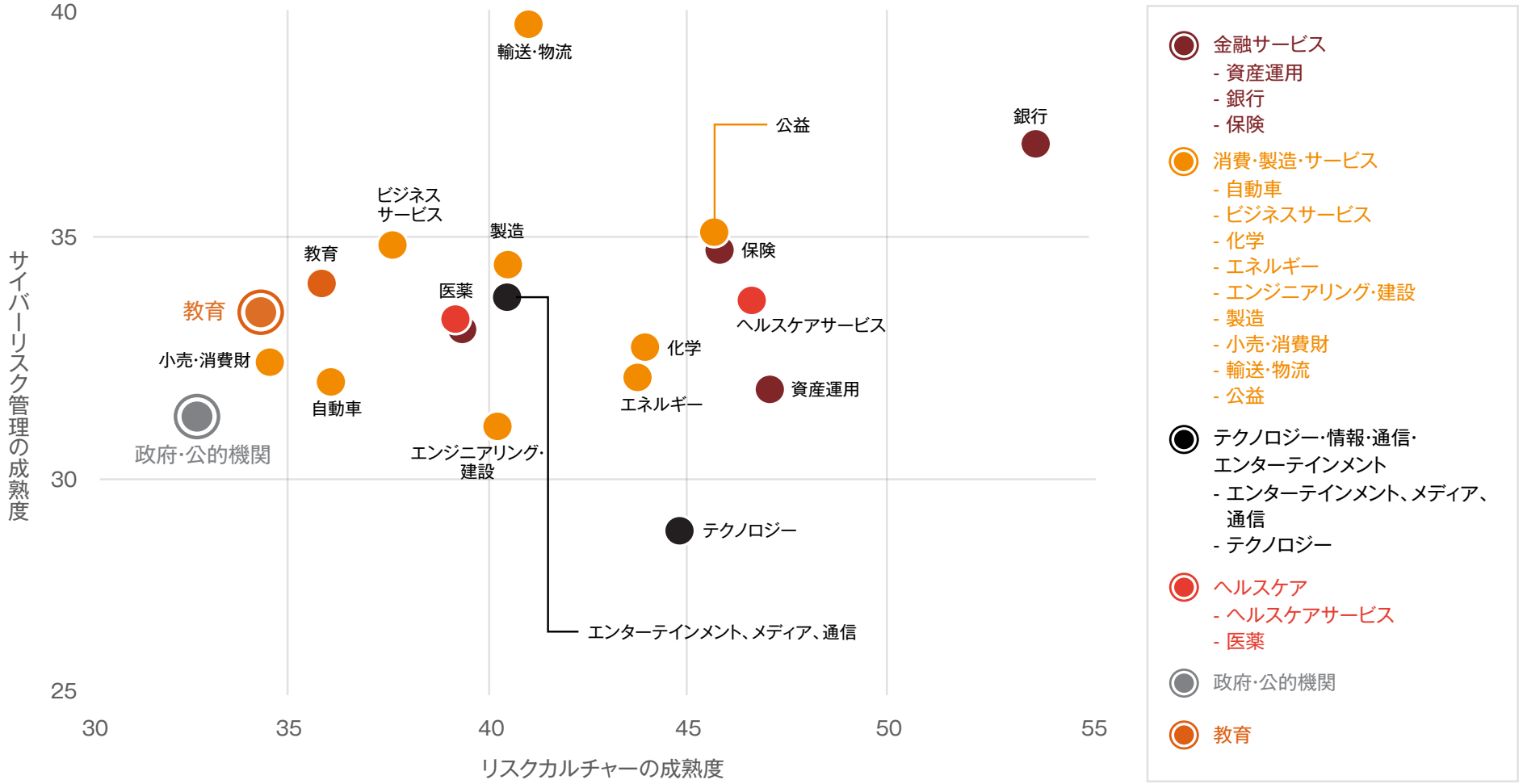
リスク管理の成熟度の測定

各セクターの相対的なリスク成熟度を検討したところ、予想されたとおりの結論が得られた。それは、「最も規制の厳しい業界では最も高度化されたリスク管理実務が導入されている」というものだ。ところが、サイバーリスク管理とリスク管理カルチャーに関する成熟度カーブに沿って主要なセクターをプロットしたところ、次ページに示すように、サイバーリスク管理の成熟度が相対的に低いセクターでは、あまり予想されていなかった可能性のある結果が導かれた。

主要なセクターグループのリスクカルチャー成熟度



さまざまな業界におけるリスクカルチャーの成熟度(横軸)とサイバーリスク管理の成熟度(縦軸)の関係



ビジネスへの提言

最適化されたリスク管理エコシステムの構築

第1ディフェンスラインのリスク管理リーダーシップとはエンゲージメントの問題、すなわち「効果的なリスク管理プログラムを構成するさまざまな要素（戦略との整合性、専門知識、プロセス、保証）に関する責任を、それを遂行する準備が完全に整ったディフェンスラインにいかに割り振るか」という問題である。それぞれのディフェンスラインの役割を明確化するということは、本来は他のディフェンスラインが実行すべき業務を引き受ける事態をなくすことにも繋がる。ライン間の緊密な連携によって、多様な視点とアイデアが生まれる自由で好ましい流れが促進される。

「リスク管理責任を第1ディフェンスラインに移管し、第2ディフェンスラインに監視の役割を担わせるためには、多くの協同的取り組みが必要だ。しかし、協同的取り組みと効果的な問題点の指摘の両立が困難な場合もある。また、リスク管理は、かつて数値データの分析を中心とする機能だった。ところが今では、効果的なリスク管理者となるには情緒的な知性も備えることが求められる。人を責めたり、対話を閉ざしたりすることなく、考え方や想定に異議を唱えられるようになる必要がある」とFannie MaeのExecutive Vice President兼CROのH. Johnson氏は指摘する。

行動を起こす

リスク管理活動の第1ディフェンスラインへの移管は、より先見的で戦略に整合したリスク管理プログラムへの移行における一つの側面にすぎない。現在の課題に合わせて最適化されたリスク管理エコシステムを構築するには、全社的な賛同が必要となる。以下、組織が正しい道を進むことを可能にする五つのステップを紹介する。

1. 組織としてリスクカルチャーへの強い取り組み姿勢を打ち出す

CEOと取締役会はリスクカルチャーへの強い取り組み姿勢の模範を示すべきである。トップの姿勢を組織に浸透させ、継続的なモニタリングと有効性の測定を実施しなければならない。

- CEOは業績管理とインセンティブがリスクカルチャーの目標と整合するようにする
- リーダーシップチームは明確で一貫したメッセージの発信を続ける
- リスクが日常的な会話や意思決定の中で意識されるようにする

2. 意思決定の際にリスク管理と戦略を整合させる

- 第1ディフェンスラインは、組織の戦略を見通すことにより、意思決定と行動を整合させるための共通のビジョンを構築し、リスクと障害に素早く対応する体制を整えることが可能になる
- 意思決定者はリスク管理を戦略立案と戦術実行の両方に組み込むべきである

3. 三つのディフェンスラインの間でリスク管理プログラムを再調整する

パフォーマンスを最適化するには、第1ディフェンスラインがビジネスリスクに関する意思決定を担い、第2ディフェンスラインが第1ディフェンスラインを監視し、第3ディフェンスラインが客観的な監督を行うことが必要である。

- 三つのディフェンスラインの境界を定義し、それに伴う必然的な共通業務を明確化することで、効果を最大化しながら役割と責任を調整することが可能になる
- それによりリーダーシップはリスクをより明確に定義したうえで各ディフェンスラインにアサインすることが可能になり、その結果としてリスクが適切な部署で管理されるようになる
- それぞれのディフェンスラインは、有効に機能するために必要な情報と人材を獲得できなければならない

4. 明確に定義されたリスク選好とそのフレームワークを組織全体に導入する

- (a)企業が事業の過程で取るリスク、(b)許容できないリスク、(c)測定・モニタリングすべきリスク、(d)戦略の達成を阻む可能性のある財務パフォーマンスの変化を伴うリスク、をそれぞれ定義する
- リスクの分類に関する共通の理解に基づいてリスクの集約・記録・予測プロセスを構築する。また、プロセスはテクノロジーとデータ分析を可能な限り活用すべきである
- リスク選好とそのフレームワークは意思決定者に明確に伝達されなければならない

5. 経営陣と取締役会による効果的なリスク監督責任の遂行を可能にするリスクレポーティングの仕組みを構築する

- リスクレポーティングの取り組みを下支えするデータガバナンスおよびデータ収集プロセスを整備する
- ビジネスの意思決定を合意されたリスク選好とリスク許容度の範囲内にとどめるためには、リスクの集約・記録・報告が不可欠である
- レポーティングとモニタリングのプロセスにおいて、リスクとそれに関連するリスク管理活動を日常的に記録すべきである
- リスクオーナーには最も重要な全社的リスクをアサインし、期限を定めた詳細なリスク行動計画の策定を要求するべきである

C-suiteが積極的な役割を担う

リーダーがリスク管理を推進する時、その行動はオーナーシップの支援にとどまらない

Chief Executive Officer（CEO）は積極的なリスクカルチャーに対する姿勢を打ち出し、組織全体の明確なリスク選好フレームワークを構築し、リスク管理と戦略立案を整合させなければならない。

Chief Financial Officer（CFO）は各ディフェンスラインと意思決定ポイントに人材を配置することでリスク管理における意思決定の調整をサポートするべきである。

Chief Risk Officer（CRO）は活発なモニタリングの促進、リスク許容度研修の主導、CIO／CISOと連携した組織全体のサイバーリスク管理を行うことにより、効果的なリスク管理を可能にする。

Chief Compliance Officer（CCO）は、組織のリスク集約のサポート役として中心的な役割を担う。CCOは他の役職の幹部よりも「会社全体のリスクを集約するための正式なプロセスを有しており、定義されたリスク選好に照らし合わせて結果を確認している」と述べる傾向が強い（CROの51%に対してCCOは58%）。

全てのテクノロジーリスクオーナーである**Chief Information Officer（CIO）**は、ディフェンスラインがリスクを予測しモニタリングするために必要なテクノロジーを準備する。**Chief Information Risk Officer（CIRO）**はCROと協力してサイバーリスクとデータプライバシーリスクをモニタリングする。

Chief Audit Executive（CAE）はリスクに対する最後の客観的なディフェンスラインとして、CROの有効性を含めてリスク管理プログラム全体を継続的に評価するとともに、第1および第2のディフェンスラインのリスク管理活動を独立した立場で評価しなければならない。

取締役会は、CEOがトップダウンのリスクカルチャーを打ち出し、集約されたリスクを組織のリスク選好とリスク許容度のフレームワークに照らし合わせて監督するのを支援する。

お問い合わせ先

PwCあらた有限責任監査法人
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
TEL：03-6212-6800（代表）

出口 眞也
製造・流通・サービス担当内部監査サービス責任者
パートナー
shinya.deguchi@pwc.com

駒井 昌宏
金融ビジネス担当内部監査サービス責任者
パートナー
masahiro.m.komai@pwc.com

久禮 由敬
製造・流通・サービス担当
パートナー
yoshiyuki.kure@pwc.com

Shaun Willcocks
製造・流通・サービス担当
パートナー
shaun.s.willcocks@pwc.com

辻田 弘志
金融ビジネス担当
パートナー
hiroshi.tsujita@pwc.com

井坂 久仁子
製造・流通・サービス担当
ディレクター
k.isaka@pwc.com

高木 和人
製造・流通・サービス担当
ディレクター
kazuto.takagi@pwc.com

本多 守
製造・流通・サービス担当
ディレクター
mamoru.honda@pwc.com

和泉 義夫
製造・流通・サービス担当
シニアマネージャー
yoshio.izumi@pwc.com

白髭 英一
製造・流通・サービス担当
シニアマネージャー
eiichi.shirahige@pwc.com

佐々木 康之
製造・流通・サービス担当
シニアマネージャー
yasuyuki.y.sasaki@pwc.com

田中 洋範
製造・流通・サービス担当
シニアマネージャー
hironori.tanaka@pwc.com

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界157カ国に及ぶグローバルネットワークに223,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.com をご覧ください。

本報告書は、PwCメンバーファームが2017年4月に発行した『Risk in review - Managing risk from the front line』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/riskinreview
日本語版発刊年月： 2017年7月　　管理番号： I201705-2