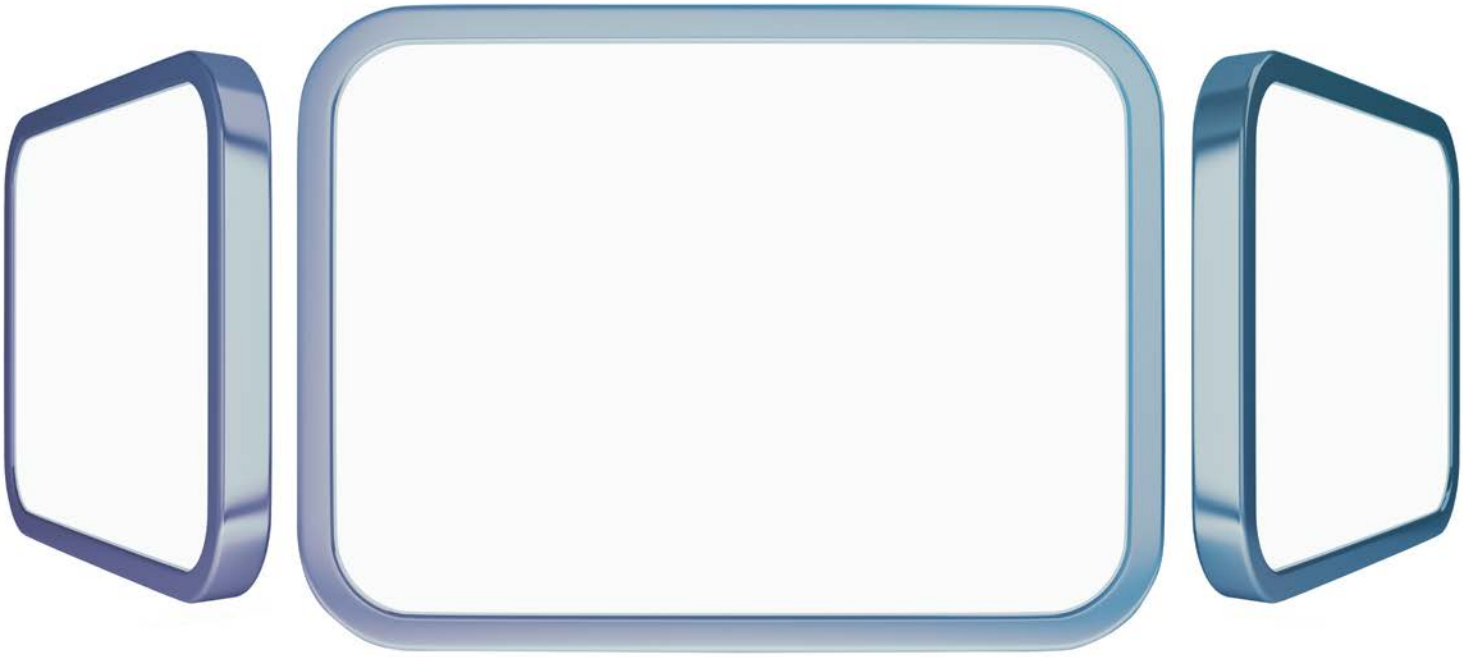
McKinsey & Company

リスク研究グループ

サイバーリスクに関するリポーティング機能の強化：リスク評価に基づくサイバー対策の導入

サイバーリスク管理システムを導入することにより、リスクを可視化し、組織の耐性を高めるとともに投資対効果の改善を図る

ジム・ベーム、ジェームス・カプラン、ピーター・メーラト、トビアス・シュテーレ、
トーマス・ポッペンシーカー、松本 拓也



2020年1月

サイバーリスクが企業にもたらす危険性について、様々な業界の経営陣の理解が深まっている。ハッキング、サイバー攻撃、データ漏洩といったセキュリティリスクが急増する今、企業全体の包括的なサイバーセキュリティ対策は取締役会における重要課題のひとつとなっている。多くの企業がビジネスモデル、コアプロセスや機密データを保護する対策を実施する一方で、各国の規制当局による個人情報に対する要件は厳格化を増している。

ヨーロッパと北米に拠点を置く金融機関の経営層に社内のサイバーリスク管理とレポーティングの現状について尋ねたところ、興味深い回答が得られた。サイバーリスク管理は、裏付けとなる事実情報が正確であることが前提であるにも関わらず、多くの企業ではサイバーリスクに関する社内のリポーティング機能が不十分であり、対策を決定するにあたり必要となる情報が得られていない、という回答だった。セキュリティ対策を担当するマネジャーは、こうした情報格差により、全ての情報資産に対して画一的な管理手法を適用せざるを得ない。その結果、優先度が低い資産が過剰に保護される一方で、重要な資産が危険にさらされている。

一部の大手企業では、サイバー攻撃への耐性を高めると同時にリスクの透明化を図り、かつそのリポーティング機能を既存システムと統合することによって効果的かつ効率的なアプローチを先駆的に導入した。

リスク管理に必要な情報が不足

多くの企業では様々なソースから取得したパッチワーク的なリポートに基づいてサイバーリスク管理が行われている。そのため経営陣にとってはサイバー対策への投資対効果を正確に評価することが困難になっている。リスクの重大性、対策の効果、および重要な情報資産の保全状態に関する情報が欠如しており、不完全で一貫性に乏しく、意思決定の根拠となるには不十分なデータしか利用できていない。加えて、サイバーリスクを管理するシステム自体を疑問視する経営陣も多く、システム導入の複雑さと結果を把握する際の煩雑さが課題となっている。

あるリスク対策の責任者は、GRC(ガバナンス・リスク・コンプライアンス)システムに対して批判的な態度を示している。このシステム導入が複雑であり長期間を要するにも関わらず、満足した結果が得られなかったことが要因だ。また他のリスク管理システムと同様に、技術者によって構築されたGRCシステムの効果を把握するには高度な専門知識が必要だったからである。ある調査では、経営陣の半数以上がサイバーリスクのレポーティング内容について、彼らの目的に対して過度に専門的であると回答している[1]。実際のところ、

[1] How boards of directors really feel about cyber security reports, Bay Dynamics, June 2016, baydynamics.com.を参照

我々はサイバーリスクを深刻に捉え、主要な情報資産を効果的に保護することが必要である。

—先端技術産業CIO

現状は混沌としている。我々には意思決定に必要な事実情報が欠如しており、この停滞した状態そのものがビジネス上のリスクを招いている。

—金融サービス企業、最高情報セキュリティ責任者

GRCシステムはサイバーリスクだけに特化したものではなく、財務、法務、自然災害、規制上のリスクを含む広範囲なリスクを網羅するものとなっている。経営陣や国の規制当局が求めるサイバーリスク管理の概観を捉えたリポーティングが機能せず、事実としてセキュリティ対策を担当するマネジャーたちの多くは、情報が不足している状態のままリスク管理を行っている。

ヨーロッパのある金融機関では、経営陣が既存のサイバーリスクに関するリポーティング機能に不満を抱き、これを改善するために以下の通り現状を評価した。

- サイバーリスクのリポートはIT技術者によってまとめられた、IT技術者のためのものであり専門性が極めて高かった。経営陣の意思決定に役立つ情報はほとんど含まれておらず、組織が直面する法務上または財務上のリスクとサイバーリスクとの関連性を把握できないため、そのリポートは全く有効ではないと判断した。
- そのリポートは期待していた内容との乖離が大きく、組織にとって最大のサイバーリスクを把握できないだけでなく、重要な情報資産、最新の事象、対策とその責任所在、脅威に対する耐性、投資対効果等に関する情報が欠如していた。
- またそのリポートはビジネス部門、ビジネスプロセス、地域や法令といった観点でまとめられておらず、システム、サーバー、アプリケーションとったIT技術に基づいて構成されており、組織全体の総合的な見解がないことから、独立した文書となっていた。

経営陣はサイバー攻撃やデータ漏洩によるセキュリティリスクの重大性を明確に把握できないばかりか、最大の脅威から重要な情報資産を守るために、何を改善すべきか理解できなかった。またそれまでに一定の緩和策は実施されていたものの、新たな対策がリスクの軽減にどのように役立つのか明確でなかった。一方でサイバーセキュリティ対策の担当マネジャーは、投資対象の重点領域を見極め、対策の正当性を役員陣に示すことが困難だと感じていた。対策全般が画一的であり、すべての情報資産に同じ管理手法が適用されていようとしていたのである。

最高情報セキュリティ責任者(CISO)は、発生したインシデントについて、問い合わせ先の担当者を把握しておらず、国の規制当局も組織情報が不十分であることを批判していた。例えば、セキュリティトレーニングを受けた従業員の割合を示す統計を拠点毎に収集していないことは、ある1ヵ国における高い参加率に対して、他国の低い参加率が見過ごされることとなりかねない。トレーニング受講率の差異により、ある1ヵ国の拠点のサイバーリスクへの危険性が高まる結果につながる。

効果的なサイバーリスクリポーティングに向けて

最先端のサイバーリスク管理には、すべての情報を集約するための情報システムが必要だ。リスクを測定する基準である重要リスク指標(KRI)により情報資産全般を評価し、重要性と脅威レベルに応じた管理手法で保護することができる。

深刻化するサイバーリスクの脅威に立ち向かうために、経営陣が率先してサイバーリスクのリポーティングおよびそのアプローチを強化することが必要である。リスクに対する重大性と複雑性に対処するにあたり、3つの目的を実現するサイバーリスク管理情報システム(MIS)を構築しなければならない[2]。

サイバーリスクの透明化: 最大の脅威と最重要な情報に対する防御策の情報を基に、専門家やIT技術者以外でも理解できる方法でリスク状況を透明化する。

リスクの概観: リスクベースで企業全体を概観し、経営層の意思決定者がセキュリティ投資を最も重要な情報資産の保護へと適切に集中させることを促す。

サイバーセキュリティ対策への投資効果: 測定可能なハイレベルの投資対効果を算出することにより対策への効率性を高める。

MISはサイバーリスクに特化しており、GRCの代替となるシステムではなく、リスクに対処するためのリポーティングソリューションである。既存システムとも連携し、IT技術者ではなく、経営層の意思決定者にとって役立つものでなければならない。経営層が脅威に対する優先度を判断し、効果的な対策を計画するにあたり、必要となる情報を取得し可視化することを目的としている。これにより、役員会議においてサイバー戦略に対する正確な情報に基づいた有効な議論と情報資産の最適な割当てをすることができる。

サイバーリスクMISは、他のITシステムのように活用方法を修得すること自体が経営陣たちの負担となってはならない。むしろ現行のビジネスインテリジェンスシステムに統合し、既存のデータソースを最大限活用できるシステムでなければならない。優れたサイバーリスクMISは、将来にわたり有効性が続くことを目的とし、最新のテクノロジーに応じた改修が可能でかつ詳細なデータソースとリスク評価についてのアルゴリズムを適宜統合できる拡張性が高いアーキテクチャ上に構築すべきである。

サイバーリスクMISのパフォーマンスを最大化するためには、各導入企業でカスタマイズすることが必要である。事実情報に基づいて、優れた意思決定を促進するシステムであるため、基本構成でも大きな効果が期待できるが、しかし経営陣はシステム導入にあたり、今後立ち向かうべきサイバーリスクのレベルについて、認識の共有を図らなければならない。

高度な分析基盤

データアナリティクスはサイバーリスクMISの基盤だ。強力でスマートな分析システムによりユーザーはネットワーク上のあらゆるソースからデータを収集し、必要に応じてリスクの分析結果を統合して俯瞰することができる。ピラミッド構造で階層的に体系化されたリスク情報が可視化されていることが理想的であり、これらのリスクデータが予想される損失インパクトの大きさ、および発生確率によって区分され示されている。また個々の部門、国と地域、資産、プロセス、建物等のKPIや対策等、より詳細な情報を必要に応じて追加することも可能であり、これらの情報には対策の導入責任者の連絡先も含まれる。

図表1に示すとおり、リスク情報を集約する際のトップダウン型アプローチには、シナリオベースの定性的なリスク評価プロセスが必要となる。必要となるデータを最小限に抑え、短期間で重要な知見が得られるトップダウン型アプローチは、最初の段階において非常

[2] Thomas Poppensieker and Rolf Riemenschnitter, "A new posture for cybersecurity in a networked world," McKinsey on Risk, March 2018, McKinsey.com.を参照

に有効な手段である。最終的には十分なリスクデータが取得できるボトムアップ型アプローチを導入する。

トップダウン型からボトムアップ型へと移行することにより、リスクの要素となる定義を明確化し、戦略決定に必要な情報を経営陣に提示するとともに、リスクの透明性とリスク緩和策の効果を高める。これらのアプローチによりサイバーリスクMISの目的を迅速に達成することができる。

図表2は「実現に向けた道筋」を示しており、優れたボトムアップ型アプローチによって導かれた緩和策により、リスクの指標を選択可能な範囲に抑えることができる。

図表1

サイバーリスク管理情報システムでは、トップダウン型のリスク収集から着手し、ボトムアップ型アプローチに移行する

リスク管理およびレポーティング

低リスク　中リスク　高リスク　最高リスク

トップダウン型のリスク情報の収集は、必要データを最小限に抑え、短期間で多くの知見が得られるため、初期段階において有効な手段である

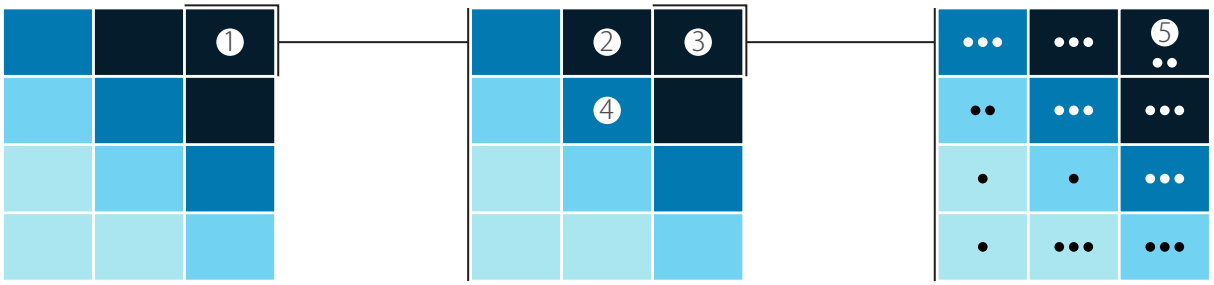
方法
- リスクシナリオをベースとした定性的かつ定量的評価

組織が成熟し必要なデータが利用可能となるにつれ、トップダウン型からボトムアップ型のリスクアプローチへと移行する

方法
- シナリオベースの定性的および定量的評価
- オペレーショナルリスク管理（ORM）手法およびポートフォリオ理論の集約

ボトムアップ型アプローチにより効果的なリスク緩和が可能となり、企業のケイパビリティに応じた予算に対し、最適なリスク対策を決定するうえで必要な領域が可視化される

方法
- ビジネスインパクト分析
- 固有および残存するリスクエクスポージャー
- リスク継承のモデリング
- ORM手法およびポートフォリオ理論の集約
- データ処理



1 グループ企業情報のリスクエクスポージャー

2 データの機密性侵害
3 データ完全性の損失
4 不十分な技術的ディザスタリカバリ

5 個別の情報資産および資産ポートフォリオのリスクエクスポージャー

レポーティング範囲

事業部門	ビジネスプロセス	資産のレベル	個別資産およびスタック	法　人	地域および国	建　物

パフォーマンスが高いサイバーリスクMISは、単なるリポーティングツールの域をはるかに上回っており、総合的な意思決定を支援するシステムとして、エンドユーザーコンピューティング、アプリケーション、インフラ、ネットワーク、建物等、すべての情報資産に関する可視性を高めることができる。経営層の意思決定者は、部門、地域、法人に関する詳細な情報を確認でき、定義、検出から、対策と評価に至るまで、サイバーリスクに対するガバナンス方針を統合的に判断することができる。

サイバーリスクMISは導入プロセスにおける設計作業が重要である。高度に集約されたスコアカードやKRIによる詳細に分析できても、経営陣が意思決定に用いることができなければ有効とは言えない。このため、優れたサイバーリスクMISには、階層の第1層や第2層の意思決定者のニーズを反映させてカスタマイズすることが重要である。

サイバーセキュリティ変革の促進

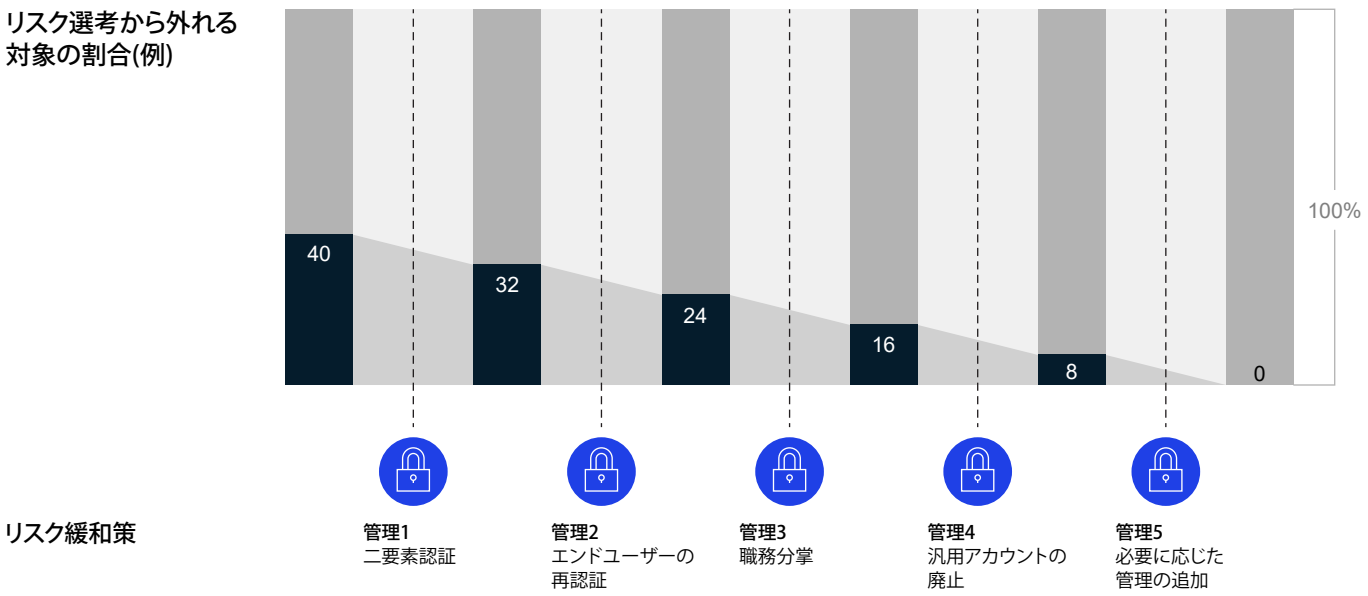
サイバーリスクMISにより包括的なサイバーセキュリティ変革を促進することが可能となる。このシステムを導入する際は、企業によるサイバーリスク関連情報の収集、および対策決定方法を変革する絶好の機会でもある。

効果的なサイバーリスクMISの導入と、サイバーセキュリティ変革は以下手順で実行される。

– 適用範囲および目的の定義: 導入リーダーは目的および成果物を事前に定義するために、まずサイバーリスク情報の収集と、経営陣による対策決定の方法を検討することが必要だ。体系的なリスクの特定および優先順位づけのための共通的な基準や最もハイレベルなリポーティング機能と体制を備えたサイバーセキュリティのガバナンスおよび組織を全社的に確立することが必要である。

図表2

ボトムアップ型集約アプローチを通してリスク緩和策を可能とする「実現への道筋」



我々はこれまでのやり方を一新するつもりはない。

我々が求めているのは、ユーザーフレンドリーなインターフェースを備えたサイバーリスク管理情報システムであり、我々固有の情報ソースから最適かつ最新のデータを抽出し統合することが必要である。

またこのシステムは効率的であると同時に、透明性を高めるものでなければならない。

—金融サービス企業、最高情報セキュリティ責任者

- 煩雑なソリューションの回避：サイバーリスクMISは1次的なものではなく、煩雑なリポートの寄せ集めと比べて分かりやすく総合的なシステムであるべき。優れたサイバーリスクMISは、様々な事業部門の成熟レベルに対応することができる。例えばモジュールが採用されているため、動的データの自動更新がされるまでの間、マネジャーは静的レポートをアップロードすることができる。MISにより意思決定者には常に最適な情報が提供される。
- 一貫性の向上：透明化を図ることで一貫性の向上につながる。変革が進むにつれ、経営陣はサイバーセキュリティとリスクに関する理解をさらに深めることが必要だ。検討すべき点は「組織として許容できるリスクの範囲と何か。また会社にとって最大の脅威とは何か。既存の資産を安全に保つために必要な防御レベルとは何か。」等である。一見些末に思えるリスクでも、有益な議論に発展する場合がある。例えばリスク警告の基準値を定義するにあたり、経営陣はリスクの選好、資産の関連性、規制要件、サイバーセキュリティの投資対効果等について、共通の見解を得なければならない。
- リスクベースアプローチへの移行：サイバーリスクMISが持つ最大のメリットは、管理におけるリスクベースのアプローチである（図表3）。「すべての情報資産を一元管理する」画一的なアプローチの代替策となり得る。リスクベースのアプローチは最も重要な資産を大規模かつ発現可能性が高い脅威から保護することに特化したものであり、意思決定者はこれに応じて投資を配分することが必要だ。これにより、サイバーセキュリティ予算を拡大することなく組織全体の耐性を高めることができる。既に導入した多くの場合、最先端のサイバーリスクMISによってセキュリティ運用費が削減されている。

ある企業ではサイバーリスクMISの実装時に構築したファクトベースの情報を用いて、段階的な管理体制を導入している。同社は最も重要かつ脆弱な資産（クラス1）のみを、多要素ユーザー認証や退社したユーザー

図表3

サイバーリスク管理情報システムを通して可能となったサイバーセキュリティ変革には、より効果的かつ低コストで柔軟性に富んだ管理体制が含まれる

サイバーリスク管理情報システムの例

- ● 管理体制が整っている
- ○ 管理体制が整っていない
- ● 管理が推奨される
- ● 適用範囲外

	 **ティア1: 管理A** 多要素認証	 **ティア1: 管理B** アカウントの再認証	 **ティア1: 管理C** 特権アクセスの中央管理	 **ティア2: 管理D** 24時間以内のアカウント無効化	 **ティア3: 管理E** データ暗号化
アプリケーション1: トレーディングシステム	●	●	●	○	●
アプリケーション2: 会計システム	●	○	●	●	●
アプリケーション3: ポリシーポータルサイト	●	●	●	●	●
脅威および管理関連の指標	KRI-KCI 1 KPI 1	KRI-KCI 2 KPI 2	KRI-KCI 3 KPI 3	KRI-KCI 4 KPI 4	該当なし 該当なし

効果的な情報セキュリティリスク管理は、重要リスク指標（KRI）、重要コンプライアンス指標（KCI）、重要業績指標（KPI）等、資産中心の指標に基づき、コンプライアンス課題や既存および予想される残存リスクエクスポージャーを明らかにするものである

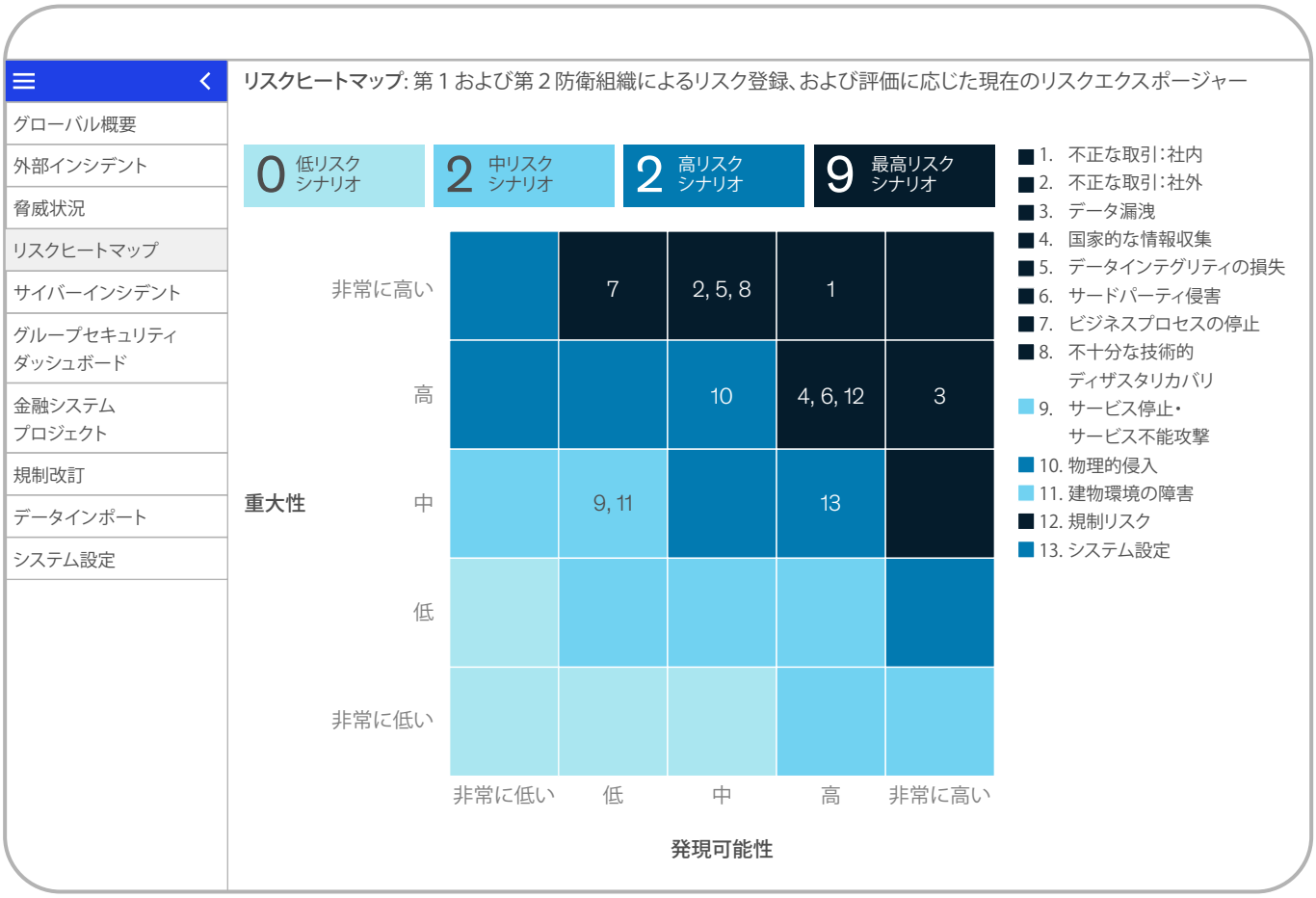
アカウントの時間後の削除等、徹底した管理対象とし、一方で重要性の低い資産には基本的な管理のみを適用した（図表3）。この段階的アプローチの結果、同社は関連する規制要件へのコンプライアンスを強化するとともに、残存するリスクレベルの引き下げに成功した。また同時に、直接コスト（ソフトウェアライセンス等）および間接コスト（低水準のアプリケーション等、既存の画一的な管理にかかっていた費用）の両方を削減している。

こうしたサイバーセキュリティ変革を通じて、あらゆるレベルの経営陣に対し、主要なサイバーリスクに関する簡潔で理解が容易な概観を提示することが可能となる。図表4はMISのサイバーリスクダッシュボードを示しており、リスクヒートマップが展開されている。最高リスク管理責任者や最高情報責任者は、あらゆる部門、組織、アプリケーションに対するKRI、KPI、管理リポートおよび進捗リポートを把握することができる。こうした変革により、組織内に共通言語ができるほか、リスクに対するファクトベースのアプローチの適用が組織全体で促進されるため、サイバーリスクの透明化、セキュリティ対策の効率化、およびサイバーレジリエンスの向上といったメリットが期待される。

図表4

リスクヒートマップが表示されたサイバーリスクダッシュボード

サイバーリスクダッシュボードの例



迅速な成果に向けて

サイバーリスクMISのモジュール構築は、組織のニーズおよび複雑性に応じた設計をすることにより、実行可能なバージョンであれば3~6ヵ月間で実装できる。多くの企業では、基礎的なデータ構造、分析基盤、可視化されたインターフェースといった重要なコンポーネントは既に整備されている。次世代型のサイバーリスクMISは、初期段階では企業全体のニーズに応じてはいないが、実際に機能する製品として有効だと言える。

導入プロセスにおいては、まずプロジェクトチーム、エキスパート、リスクマネジャー、データ責任者、ITおよびその他ステークホルダーが協力して具体的な要件や関連プロセス、データの可用性について定義することが必要だ。構築する段階ではトライアルのライブセッションを通じて、経営陣がMISの有効性に関するフィー

我々は一歩ずつサイバーリスクMISを導入した。すべてのプロセスに要したのはわずか半年未満だが、既製品ではなく当社のためのソリューションが完成した。

—サイバーリスクMISユーザー

ドバックを行う。必要な調整を経て適用範囲を拡大し、システムの組織全体への展開を計画する。

実際に、最先端のサイバーリスク管理情報システムを導入した組織は、サイバーリスクの検出および改善の効率を大幅に高めている。

このシステムはプラットフォームとして運用データと連携しグループ全体の企業リスク管理情報と正確かつ一貫したデータ連携が可能となる。これにより、総合的なサイバーセキュリティ変革の基盤や包括的なリスクベースのサイバーセキュリティアプローチが実現され、リスクの軽減、レジリエンスの強化、コスト管理に役立つことが期待される。

ジム・ベーム：アソシエイトパートナー、**ジェームス・カプラン**：パートナー（ニューヨークオフィス）、
ピーター・メーラト：アソシエイトパートナー、**トビアス・シュテーレ**：シニアエキスパート（フランクフルトオフィス）、
トーマス・ポッペンシーカー：シニアパートナー（ミュンヘンオフィス）、**松本 拓也**：パートナー（東京オフィス）

本記事の作成にあたり貢献されたロルフ・リーメンシュナイター氏に謝意を表する。