連載

非財務リスク管理 最前線

第5回

サイバーリスク定量化と活用事例

デロイト トーマツ リスクサービス
サイバーリスク担当 パートナー **野見山 雅史**

有限責任監査法人トーマツ
フィナンシャルインダストリー担当 マネジャー **加瀬 鶴佳**

サイバーリスク定量化への関心の高まり

近年サイバー攻撃による甚大な被害が相次ぎ、多くの企業がサイバーリスクを経営のトップリスクとして位置付けている。一方で、自社のサイバーリスクの評価・把握に苦慮しているとみられる。その解決の一助としてサイバーリスク定量化への関心が高まっている。

デロイトのサイバーリスク定量化のアプローチは、想定されるサイバー攻撃のシナリオを策定し、各シナリオの①損失額の推定と②発生確率の推定を独立して実施したうえで、二つの結果から③Value at Riskを計測するという三つのステップにより構成される。これは金融機関においてオペレーショナルリスクの計量化に多く用いられるアプローチと基本的に同一である。

①損失額の推定

損失額の推定は、「業務内容・業務プロセスの把握を通じた情報資産の洗い出し」と「財務情報の分析に基づく上記情報資産が毀損した場合の損失額の推定」の二つの手法を組み合わせることで実施する。

まず、情報資産情報を「機密性」「完全性」「可用性」の観点を踏まえた区分に整理し、各社のビジネスモデル・業務プロセスを把握したうえで、さらに細分化を行う。そのうえで、情報資産の区分ごとにサイバー攻撃によってこれらが棄損するシナリオを策定する。次に、情報資産が棄損した場合（シナリオ発生時）の損失額について、時価総額や売上高といった財務情報や、個人顧客数／従業員数、R&D（研究開発）投資額およびIT予算額といった経営数値を用いて推定する。

②発生確率の推定

最初に、サイバー攻撃者の想定を行う。この際、攻撃者の技術レベルが低い順に、大量妨害攻撃・マスサイバー犯罪・高度サイバー犯罪・サイバーエスピオナージ（情報通信技術を用いて政府や企業の情報を盗み出す諜報活動）といった分類を行うことが考えられる。一般的に技術レベルが低いほど攻撃を受ける頻度が高く、技術レベルが高いほど攻撃頻度は低い傾向にある。次に、攻撃者の侵入阻止および侵入された場合の検知・対応から損失発生（および回復）に至る一連のプロセス（デロイトでは「アタック・プロセスモデル」と呼んでいる）をベースに、想定した攻撃者の種類と、企業が各プロセスで設定してい

るコントロールの強度から、シナリオの発生確率を推定する。

③VaRの推計

推定した損失額と発生確率に基づいて、サイバーリスクのValue at Risk（サイバーVaR）を計測する。前記①および②で作成したシナリオの損失・発生頻度について、モンテカルロシミュレーションを実施し、損失分布を仮定し、得られた損失分布から、最悪のケース（例えば、95％点）を特定する。

サイバーリスク定量化の意義

サイバーリスク定量化の意義は、次の四つに大別できる。

①リスクの手当

万が一セキュリティ侵害が生じた場合に備えたリスク手当、すなわちサイバー保険への加入、引当金などの財務的手当の要否や必要金額について具体的な検討が可能になる。

②リスクの低減

セキュリティ対策の効果測定を定量的に行えることから、より効果的なリスク低減策の検討および選定・導入が可能になる。

③投資効率化

セキュリティ投資の効果測定を定量的に行えることから、セキュリティ投資の優先順位付けが可能になる。

④コンプライアンス

将来の規制強化への準備を行うことが可能になる。

前記のうち、特に①や③については、定量化によって具体的な数値が把握できることから、定性的リスク評価を判断根拠にする場合と比べて経営による意思決定がしやすくなり、その意義が大きいと考えられる。

④については、現時点では、サイバーリスク定量化を明示的に求める法規制は見当たらない。しかし、米国の金融規制当局（連邦準備制度理事会、通貨監督庁および連邦預金保険公社）が16年10月19日付けで規制案制定事前通告（「Enhanced Cyber Risk Management Standards」）を発表し、その中の「Ⅲ. Approach to Quantifying Cyber Risk」でサイバーリスク定量化について言及している。そのため、将来的に大手金融機関ではサイバーリスク定量化が求められる可能性も想定される。

サイバーVaRの活用事例

ある欧米大手金融機関では、サイバーVaRをセキュリティ対策の投資優先順位の判断指標として活用している。システム部門やセキュリティ部門により起案されたセキュリティ対策について、サイバーVaRによって計測されたリスク低減効果と、投資額からROIを算出して優先順位付けを行っており、投資効率の向上にも寄与している。

また、あるグローバルテクノロジー企業では、サイバーVaRをセキュリティ対策のKPIとして活用している。役員会報告用、最高情報セキュリティ責任者（Chief Information Security Officer）報告用、セキュリティ部門用のKPIをそれぞれ設定し、四半期などの頻度でダッシュボードを作成・報告する。これにより、経営層に対して、サイバーリスクと事業価値の関係、対策導入・運用によるリスク低減効果を具体的に説明することが可能になり、意思決定の効率化にも寄与している。

＊　＊　＊

サイバーリスク定量化により、経営者にそのリスクの程度を具体的数値として示すとともに、現場のシステム部門・セキュリティ部門に対して経営者との共通言語（定量化による事業価値（金額）換算）を提供することで、経営者と現場部門の橋渡しが可能になる。また、サイバーリスクはシステム部門が所管部門であることも多い一方、定量化にあたっては、事業部門やリスク管理部門の関与が必要になるため、システム部門に偏ったサイバーリスク管理態勢を見直し、組織横断的な態勢に変革するための契機にもなろう。

他方、最初から網羅的かつ高精度なサイバーリスクの定量化を行うことは、作業負荷や内部データの制約といった観点でハードルが高いため、外部データを活用するなどの簡易的アプローチで定量化を試行し、段階的に精度を上げていくアプローチが現実的であろう。まずは定量化に向けた一歩を踏み出すことが重要である。