The Josai Journal of Business Administration (2023), Vol. 19, No. 1, 11−26

コラボレーションか統合か：
効果的なサイバーリスク管理とサイバーセキュリティのための戦略

辻　智佐子・辻　俊一・足立　照嘉

要　旨

ビジネスがグローバルかつデジタル空間と相互接続された現代において，企業が生き残ると同時に持続的な成長をしていくためには攻めの経営が必要であり，効果的かつ効率的なサイバーリスク管理とサイバーセキュリティを事業戦略に組み込まなければならない。本稿では，そのための手法として以下の点を指摘した。

まず，サイバーリスク管理プロセスはリスク識別，リスク分析，リスク対応，リスクモニタリング，リスクコミュニケーションと報告の５つのステップで構成され，従業員教育や組織内コミュニケーションとのコラボレーションが重要である。次に，現在のサイバーリスク管理には課題と限界もあり，脅威の急速な進化，システムの複雑性と相互接続性の向上，従業員による理解，予算の制約，優先事項のバランス，熟練したサイバーセキュリティ専門家の不足，コンプライアンスとガバナンスの実現といったことがあるが，他の企業や政府機関と協調したリスク管理によって効果的かつ効率的に対応していく必要がある。

キーワード：サイバーリスク管理，サイバーリスク評価，サイバーセキュリティ文化，持続的成長，事業継続

1. 問題提起

日本企業を取り巻く環境は刻一刻と変化しており，そのスピードは速い。加速する経済のグローバル化に加え，いまや企業の経済活動に不可欠となった情報技術の目まぐるしい進展は，大企業のみならず中小零細企業の経営にも大きな影響を及ぼしており，企業が存続・発展していくためには柔軟な対応をもって自らを変化させていくことが肝要である。

日本は，戦後から 1990 年頃まで第二次産業を主軸として右肩上がりの成長を遂げてきた。その過程で「日本的経営」が確立し，主にアメリカが辿った経済発展のレールに乗って時代に適した経営ノウハウを構築してきた。しかし，それは昔の話である。多くの企業はいまだにそのレールから降りようとせず，かつての経営ノウハウにしがみつき，後ろ向きの姿勢で「失われた 30 年」を過ごしてきたように思われる。厄介なことに，この 30 年で社会はデジタル化し，それ以前よりも早いスピードで変化し始めた。一方で，この間にアメリカやドイツ，そしてかつては眠れる獅子と呼ばれた中国など，現在の世界経済を牽引している国々は，ロールモデルのないグローバル・デジタル時代に挑戦し続け，日々変化している。変化は成長の要件であり，変化に必要なのは企業の前向きの姿勢であり，攻めの経営である。

攻めの経営には，例えば，事業のグローバル化や多様な人材の活用，イノベーション創造に向けた積極的な投資などいくつもの選択肢があるが，企業によってはすでに着手している内容であろう。それでも日本企業が概して新たな挑戦や変化に及び腰であると言えるのは，リスクに対する消極的な考え方に

あり，またリスクをチャンスに転換する発想の欠如にある。

企業が対応しなければならない経営上のリスクはさまざまにあり，前稿で述べたように，一般には企業の外部環境におけるリスク（政治，経済，社会，技術に係るリスク）や内部環境におけるリスク（人，モノ，カネ，情報に係るリスク）が挙げられる（辻他［2022］2-3 頁）。しかしここで着目するリスクは，これらのリスクと繋がり，包摂して影響を与えるサイバーリスクである。サイバーリスクは，国や地域の歴史や文化，言語などに左右されないため，その対応は複雑であり，専門的な知識や技能を必要とする。日本の現状では，サイバーリスクから企業を守ることに主眼を置いた対策が比較的規模の大きな多国籍企業を中心に進んでいるが，グローバル・デジタル時代の現在，攻撃する側はより効率的に甚大な被害を与えることができ，そのスピードは速いため，サイバーリスクに対する守りの体制では打開策のない千日手となり，企業は疲弊していくばかりである。前稿で提起したように，サイバーリスクを「危機」ではなく「機会」として捉え，サイバーセキュリティ対策を戦略的リスクマネジメントに組み入れることが緊要であり，世界の視点から見ると今やコモンセンスとなりつつある(1)。

しかし，多くの日本企業はサイバーリスクにおいて後塵を拝しており，それは間違った認識からきている。1 つに，「過去にサイバー攻撃を受けたことがない」，「サイバー攻撃を受けるような組織ではない」という認識のもとで，自らが直面している潜在的なリスクに関心を持とうとしない(2)。しかし，情報技術に依存している企業はその規模にかかわらずサイバー攻撃の対象であり，仮に攻撃を受けた場合の潜在的な影響は計り知れない(3)。

2 つに，「サイバーセキュリティは技術的な問題である」という認識である。サイバーセキュリティは IT 部門の仕事であり，技術的な問題であるという認識がいまだに広く共有されている。IT 部門はサイバーリスクの管理において重要な役割を担うのは当然だが，サイバーリスクは経営全体の問題であり，この問題にうまく対処するには組織内の協力と協調が必要である。効果的なサイバーリスクの管理には，技術的な解決策を講じるだけでなく，人材配置やプロセス，ガバナンスを考慮した企業全体のアプローチが不可欠である。

3 つに，「リスクマネジメントに充てる余裕がない」，「他に優先すべきことがある」という認識から生じるリソースの不足である。効果的なサイバーリスクの管理には，人，モノ，カネといった経営資源の大幅な投資が欠かせない。留意すべきは，サイバー攻撃のコストは，効果的なサイバーリスク管理を実施するためのコストよりもはるかに高くなる可能性があるということだ。加えて，企業のサイバーリスクへのエクスポージャーを大幅に低減できる費用対効果の高い解決策が数多く存在することは，あまり知られていない。

4 つに，「既存のセキュリティ対策で十分である」という認識である。企業によっては，サイバーリスクから身を守るには，既存のセキュリティ対策で十分だと考えている。しかし，サイバー脅威は常に進化しており，過去に有効であった対策が現在も有効であるとは限らない。企業は，脅威が変化する中でセキュリティ対策が有効であることを確認するために，定期的にセキュリティ対策を評価しなければならない。

サイバーリスクに対する消極的な姿勢を是正するには，まず教育をとおして従業員のサイバーリスクに関する理解を深め，意識を向上させることである。この教育は，IT 部門の従業員だけを対象とするのではなく，すべての部門の従業員に拡大しなければならない。学びの材料には，例えばサイバーセキュリティを戦略的リスクマネジメントに転換している企業のケーススタディやサクセスストーリーの参照がある。さらに，専門家の助言を求めたり，関連する業界団体に参加したりすることも有益であ

る。学びによる意識の向上によって，サイバー上の潜在的なリスクとそのリスクを管理するために誰もが果たすべき役割について認識を深め，サイバーセキュリティに対する感度の高い企業文化を創造することができる。

そのために必要なのが，組織内の円滑なコミュニケーションによる協力体制の構築である（Hooper and McKissack［2016］）。IT 部門だけでなく，例えば法務部や人事部などサイバーセキュリティに直接関わる部門のステークホルダーの協力によって，企業は経営のあらゆる側面を考慮したサイバーリスク管理への全体的なアプローチを開発できる。こうした日々の積み重ねの上に，企業は初めてサイバーリスク管理の優先順位を決め，これらの管理に必要なリソースを最適に割り当てられる。

本研究は，日本企業がサイバーリスクに対する認識を改め，上記のような活動をルーチンとして行い，サイバーリスクに対する攻めの経営を行えるように，サイバーリスクを戦略に置き換えていくには経営者はどのような選択と意思決定ができるかについてロードマップを提示することが目的である。その入口として本稿では，第 2 節でサイバーリスク管理の定義とその重要性，そしてアプローチとプロセスについて述べ，第 3 節でサイバーリスク管理のプロセスで生じる課題と限界，その対策について事例を引用しながら論じる。

2. サイバーリスク管理とその重要性

情報技術の進歩とデジタル化の進展に伴い，企業や個人が直面するサイバーリスクは複雑化・多様化しており，サイバーセキュリティに関する意識と関心が高まっている。例えば，データ漏洩，ハッキング，不正アクセス，悪意のあるソフトウェア，そして，従業員による情報の不正取得，サプライチェーンリスクなどが挙げられる。コロナ禍以降，ビジネスのオンライン化が進み多くの企業や組織では，オンラインでのビジネスやリモートワークに移行したことで，大量の機密情報をオンライン上でやり取りする必要が生じている。これらのリスクは，企業や個人にとって大きな損失をもたらす可能性がある。サイバーセキュリティを確保するために，サイバーリスク管理が必要不可欠となっており，サイバーリスクを軽減するためのセキュリティ対策，リスク評価，社員教育，定期的な監査といった手段を講じることや，事業継続計画（BCP）や災害復旧計画（DRP）の策定によってサイバー攻撃に備えることも重要である。組織がサイバーリスクに対して十分な対策を講じることで，事業継続性を確保し，信頼性の高いサービスを提供することができる。

サイバーリスク管理とは，サイバー空間における脅威から資産を保護するために企業や組織が導入する戦略とプロセスを指す（Gonzalez-Granadillo et al.〔2021〕）。そして，サイバーリスク管理には，サイバーセキュリティ対策を用いてサイバー攻撃を予防・検知・対応すると共に，悪用される可能性のあるリスクを軽減することも含まれる。サイバーリスク管理における従来の取り組みでは，サイバーセキュリティの文化・意識とトレーニング，サイバー攻撃の影響と軽減，サイバーリスク管理プロセスなどの特定の側面に対して個別に焦点を当ててきた。

近年，企業のデジタル変革が急速に進んでいることから，モバイルデバイス，クラウドサービス，ソーシャルメディア，IoT などの変革によって貴重な資産や機密情報を保護するための堅牢なサイバーセキュリティの必要性が増しており，サイバーリスク管理の重要性が一層高まっている。このことから，企業におけるリスク管理の主な焦点にサイバーセキュリティも含まれるようになってきた。サイバーリスク管理をエンタープライズ・リスク管理フレームワークに統合することを検討し，サイバーリ

スク管理の実践をビジネス目標に合わせて調整して，サイバーリスクを総合的かつ包括的に管理できるようになる。

世界経済フォーラム（World Economic Forum）では，2019 年の世界のリスク要因トップ 5 の一つとしてサイバーセキュリティを挙げており，企業や組織がサイバーリスク管理能力を強化することを提唱している。企業は，戦略的・戦術的・運用的なアプローチによって，サイバーリスクへの対応を計画的かつ効果的に行わなくてはならない。また，サイバーセキュリティに関する従業員の意識と関心を高めるために適切なトレーニングを提供することで，サイバーセキュリティ対策をより強固にすることができる。

サイバーリスク管理とサイバーセキュリティの向上は潜在的な攻撃から組織を保護するだけでなく，消費者からの信頼や収益機会も高めることにも繋がる（Kejwang〔2022〕）。サイバーリスク管理は，企業が信頼性と完全性を維持し，法規制を遵守し，最終的には組織の持続的成長へと繋がるために必要な活動である。これには，従業員や顧客のデータの保護，事業継続性の確保，リスクマネジメントの改善，サプライチェーンの保護などが含まれる。

サイバーリスクが管理されていない場合，組織は重大な損失を被る可能性があり，その損失は直接的な財務的損失（罰金や訴訟費用など），顧客やパートナーとの信頼の喪失，ブランドイメージの毀損，そして最悪の場合には組織の存続にすら影響を及ぼす可能性がある。例えば，クリプトジャッキング，クラウドコンピューティングを介したデータ漏洩，高度持続的脅威（APT），セキュリティの不十分な IoT 機器を介したネットワークの侵害，EU 一般データ保護規則（GDPR）などのプライバシー規制の遵守不足，フィッシング，ウェブサイトへの攻撃，盗まれた資格情報の悪用などが，組織が直面する可能性のある脅威の一部として挙げられる。

効果的なサイバーセキュリティの実践には，サイバーリスク管理を優先し，必要なリソースを割り当てることが不可欠である。サイバーリスク管理によって適切なリソースを割り当てることで，組織に必要なサイバーセキュリティ対策を実装し，定期的にリスク評価を実施し，最新の業界トレンドやベストプラクティスを常に把握することができる。このような積極的なアプローチは，組織が潜在的な脅威を回避し，サイバー攻撃による影響を最小限に抑えるのに役立つ。

サイバーリスク管理のアプローチとしては，戦略的・戦術的・運用的なアプローチを採用することが必要である。戦略的なアプローチでは，組織全体のサイバーリスクを軽減するための準備度を評価していく。この評価には，組織の属する産業，IT の設定状態，関連する法規制，労働力の地理的な分散など，組織の文脈と要素が考慮される。戦術的なアプローチでは，組織内で運営する部門やビジネスユニットのセキュリティ要件を評価し，潜在的なリスクがビジネス目標を阻害する可能性を減らしていく。運用的なアプローチでは，IT アプリケーションやソリューションへのサイバー攻撃から耐えられるように，サイバーセキュリティのレジリエンスを構築していく。また，サイバーリスク管理には，人的要因も重要な役割を果たす。従業員の教育・訓練，セキュリティ文化の定着，組織全体の意識向上などが必要となる。これらのアプローチを組み合わせ，脅威プロファイルを作成するために必要な情報を収集し，サイバーリスクを管理して，サイバーリスクを最小限に抑えていく。

そして，サイバーリスク管理を効果的に実現するためには，サイバーリスクについて従業員教育を実施し，意識を向上させることも不可欠である。トレーニングプログラムや意識向上キャンペーンを通じて，従業員はサイバーリスクをより深く理解し，潜在的な脅威を特定して対応する方法を学ぶことができる。そして，サイバーリスク管理に不可欠な組織内における円滑なコミュニケーションに対しても，

従業員への教育や意識向上によって，さまざまな部門間の調整とコラボレーションが向上し，全員が潜在的なリスクを認識し，協力しての対処ができるようになる。

サイバーリスク管理の実践として，まずはサイバーリスク管理の定義・種類・影響について理解する必要がある。そして，完全性・可用性・機密性に関連したリスクを特定・評価・対応していく。これには悪意のある攻撃・データ侵害・内部関係者による脅威といったサイバー空間における脅威から，機密データ・システム・ネットワーク・インフラストラクチャを保護することが含まれる。

サイバーリスク管理が効果的なものではなかった場合，その影響は組織にとって深刻かつ莫大なコストを生じさせる可能性がある。サイバー攻撃は経済的損失や風評被害を引き起こすだけでなく，法規制に伴う罰則や顧客からの信頼と忠誠心の喪失，事業中断に繋がる可能性もあるからだ。そのため，企業は体系的なプロセスに従ってサイバーリスクを効果的に管理する必要がある。そして，このサイバーリスク管理のプロセスは，リスク識別・リスク分析・リスク対応・リスクモニタリング・リスクコミュニケーションと報告の５つのステップから構成される。それぞれのステップは異なる目的を持ち，組織によっては特定のステップにより多くの時間を費やす必要がある場合がある。

1） リスク識別

組織のIT資産を脅かす可能性のある潜在的なサイバーリスクの特定。これには潜在的な脅威の特定，それらが標的とする可能性のある情報資産の特定，脅威によって資産を損なう可能性のある脆弱性の特定が含まれており，組織のシステム・ネットワーク・データのライフサイクルにおけるさまざまな段階にわたって詳細に評価し，脆弱性や潜在的に攻撃可能な箇所を特定していく。ここでの情報を基に企業はリスクプロファイルを作成し，どのようなリスクに対して最も脆弱であるかを理解することができる。リスク識別は，サイバーリスク管理の基礎である。

2） リスク分析

リスクが特定されたら，その可能性と組織に対する潜在的な影響の観点からリスクの重要度を評価する。これは各リスクの可能性とその影響を評価することによって行われ，特定のリスクが発生する確率を求め，そのリスクが発生した場合の潜在的な損害や影響を示す。これらの要素からリスクスコアを計算し，どのリスクが最優先で対処されるべきかを決定するのに使用できる。リスク分析はリスクプロファイルのより詳細な理解を提供し，リスクの軽減に向けたアクションプランを立てるための重要なステップである。

3） リスク対応

リスクを評価したら，組織はリスクへの適切な対応方法を決定する必要がある。これには特定されたリスクを軽減するためのセキュリティコントロールの実装，リスクを受け入れる決定，リスクを他のパーティーに転嫁する（例えば，保険を購入する），リスクを完全に回避する（例えば，特定の業務活動を中止する）ことが含まれる。セキュリティコントロールの実装とは，具体的にはファイアウォール，暗号化プロトコル，多要素認証などのセキュリティ対策の実装を含む。リスク対応ではリスク許容度・リソース・戦略的目標に基づき，企業はリスクを軽減しセキュリティ上の脆弱性を低減することができる。 また，発生する可能性のあるサイバーインシデントを効果的に処理し封じ込めるためのインシデント対応計画を確立する必要がある。インシデント対応計画にお

いては，サイバー攻撃またはデータ侵害が発生した際に迅速かつ効果的な行動を確保するための対応手順について，明確に定義されたインシデント対応計画を確立する。これには，影響を受けたシステムの隔離，インシデントを調査して原因と範囲を特定すること，将来の発生を防ぐための対策の実施，バックアップおよびリカバリ戦略が含まれている必要があり，役割と責任の明確な定義，通信プロトコルの確立，即応性を確保するための定期的なトレーニングと演習の実施が含まれる。

4) リスクモニタリング

サイバーリスク管理は継続的なプロセスであり，サイバーリスク管理プロセスを継続的に監視し，新たに識別されたリスク，変化する脅威の状況，リスク対応策の効果と有効性に対応していく必要がある。これにはリスク評価の定期的な更新，セキュリティコントロールの効果的な運用を確認するための監査，リスク管理計画の更新が含まれる継続的な改善と最適化を促進するための重要なステップであり，サイバーリスク管理戦略を変化し続ける IT 環境とサイバーリスクに適応していくことができる。

5) リスクコミュニケーションと報告

リスクコミュニケーションと報告は，組織内の異なる部門や利害関係者との協力を促進し，リスク管理の透明性を高めるための重要なステップである。これによってリスクに関する理解を共有し，リスク管理活動の透明性を確保し，必要な場合には追加のリスク対応措置を講じることができる。

これら５つのリスク管理プロセスのステップは，サイバーリスク管理における戦略的・戦術的・運用的なアプローチの一部として実施することができる。戦略的なアプローチでは組織全体の準備度を評価し，リスク識別と評価を通じて脅威プロファイルを作成する。戦術的なアプローチでは，組織内の部門またはビジネスユニットが運営するセキュリティ要件を評価する。運用的なアプローチでは，IT アプリケーションやソリューションに対するサイバー攻撃に耐えるためのセキュリティのレジリエンスを構築する。これらのアプローチを組み合わせることで，組織はそのサイバーリスクを適切に管理し，そのビジネス目標を達成する能力を強化することができる。

リソースの割り当てには予算と人員の割り当ても含まれており，従業員の教育と意識向上プログラムへの投資，高度なサイバーセキュリティ技術やツールへの投資，サイバーセキュリティ分野の熟練した専門家の採用，従業員に対する継続的なトレーニングや教育などに予算を割り当てる場合がある（Nan et al.〔2022〕）。

そして，サイバーリスク管理とサイバーセキュリティ対策の実施に加えて，サイバーリスクについて従業員を教育し，意識を向上させることが不可欠である。これまでに発生してきた多くのサイバーインシデントでは，意図的なものであるか否かにかかわらず，従業員が組織内で最も弱い存在となってしまったことが多い。したがって，サイバー空間における脅威とサイバーセキュリティのベストプラクティスについての教育をすることが重要である。これには，フィッシングに対する認識，パスワード管理，安全なブラウジングの実践をカバーする包括的なトレーニングプログラムを通じて実現できる。

また，従業員には，遭遇する可能性のある不審な活動や潜在的なセキュリティ侵害を報告するよう奨励する必要がある。オープンなコミュニケーションの文化を育み，明確な報告チャネルを提供すること

で，組織は，従業員がサポートされていると感じ，企業のサイバーセキュリティを強力に保つために従業員が積極的な役割を果たす環境を作り出すことができる。

さらに，組織は円滑なコミュニケーションとコラボレーションを促進する協力体制を確立する必要があり，部門間の情報共有が促進されることで，サイバーリスク管理において部門を超えた協力と連携が促進される。効果的なコミュニケーションとコラボレーションを通じ，組織は関連するすべての利害関係者がリスク管理プロセスに関与し，サイバー脅威に関する情報が組織全体に迅速かつ効果的に伝達される状態を確保する。ただし，サイバーリスク管理のために効果的なフレームワークは，組織の規模や業種における要求や要件などによっても異なるため，自組織に適したフレームワークを検討する必要がある。

サイバーリスク管理は企業活動においてもはや不可欠な活動であり，適切な戦略的・戦術的・運用的なアプローチを採用し，最新の情報を把握しながら，常に最適な対策を講じることが求められる。増加の一途を辿るサイバー攻撃に加えて近年では，AI（人工知能）や IoT（モノのインターネット）などの技術の進歩によって，サイバーリスクはより複雑なものとなっている。これらの技術は，組織の IT 資産をより広範囲に渡って管理し，サイバー攻撃の標的にされる可能性が高まっている。そのため，組織は新たな技術に対する適切なセキュリティ対策を講じる必要がある。

また，サイバーリスク管理には，国際的な法規制が適用されることもある。例えば，EU 一般データ保護規則（GDPR）は，個人データの取り扱いに関して EU 域内在住者の個人データを取り扱う企業に適用される重要な規制である。GDPR には，個人データの取り扱いに関する規定が明確に定められており，企業はこれらの規定に従って，適切な個人データの保護を行う必要がある。サイバーリスク管理においては，常に最新の情報を把握し，適切な対応策を取ることが重要である。組織は，サイバーリスク管理に関する情報やトレンドを定期的に調査し，最新のセキュリティ対策を講じる必要がある。また，サイバーリスク管理に関する情報を組織内や組織間で共有することによって，組織全体でサイバーリスクに取り組まなくてはならない。

そして，サイバーリスク管理のプロセスによって組織のセキュリティ状況を改善し，継続的な事業活動を支援し，評判を保護し，コスト削減に役立ち，事業継続性と持続的な成長を支援することへと繋がる。

3. サイバーリスク管理プロセスの課題と限界

サイバーリスク管理の効果的な実践と資産の保護には，企業におけるサイバーリスク管理への積極的かつ戦略的なアプローチを採用する必要がある。そこには，ビジネス同様に，サイバー攻撃やインシデントに関連するリスクを予見および評価し，サイバー攻撃に対する組織の体制と準備レベルをシステムのライフサイクルのさまざまな段階を考慮して評価するプロセスが含まれる（Rosa, Maunero, Prinetto, Talentino and Trussoni〔2022〕）。ただし，効果的なサイバーリスク管理戦略を導入するプロセスには，課題や限界がないわけではない。以下は，企業が直面する主な課題や限界である。

1） 脅威の急速な進化

サイバーリスク管理プロセスにおける課題の１つは，サイバー空間における脅威の急速な進化である。サイバー攻撃者は脆弱性を悪用し，セキュリティ防御を突破するための新しい手法やテクノ

ロジーを絶えず開発している。このため，企業は警戒を怠らず，新たな脅威に対処するためにサイバーリスク管理戦略を継続的に更新する必要がある。例えば，高度なフィッシング攻撃やランサムウェアの台頭により，組織はリスク評価と軽減策を強化することが求められており，例えば2021年のランサムウェア攻撃によるColonial Pipelineへのサイバー攻撃では，ガソリンの供給が中断したことによって一部の州ではガソリンスタンドのガソリンの枯渇や，飛行機の飛行ルート変更などが余儀なくされ，推定4.4億ドルの損失が発生したとされている。

2） システムの複雑性と相互接続

企業内のITシステムとネットワークが相互接続されさまざまなテクノロジーと依存関係にあるため，複雑性は増し続けており，潜在的な脆弱性をすべて特定して，その影響を正確に評価することが困難となっている。さらに，サイバー攻撃による潜在的な攻撃対象領域も増大している。例えば，2017年に発生した米国最大の信用調査機関の1つであるEquifaxにおいて，数百万人もの消費者の個人情報が流出する大規模なデータ侵害が発生した。この侵害はシステム内の既知の脆弱性の特定とパッチ適用に失敗したために発生した。これは，複雑で相互接続されたテクノロジー・インフラストラクチャ全体でリスクを効果的に管理することの難しさという課題を浮き彫りにした。また，もう1つの例として，2018年にアトランタ市に対してランサムウェア攻撃が発生した。この攻撃により，いくつかの市のサービスが麻痺し，市は復旧作業に数百万ドルの費用を費やした。ここでも，組織はますます複雑かつ進化するサイバーセキュリティ環境の中で，サイバーリスクを管理するという課題に直面している。加えて，サードパーティのベンダーやサプライヤーへの依存によって，リスク管理がより複雑なものとなっている。近年では取引先や関連会社などからもたらされるサードパーティのリスク，もしくはサプライチェーンリスクが深刻な問題となっている。例えば，2022年にトヨタ自動車のサプライヤーである小島プレス工業で発生したランサムウェア攻撃による被害では，同社とシステムを連携しているトヨタ自動車にも影響がおよび，小島プレス工業がサイバー攻撃被害を受けた翌日にトヨタ自動車の日本にある全ての工場が操業停止を余儀なくされた。そのため，ベンダーやサプライヤーにも堅牢なサイバーセキュリティ対策を講じていることを確認する必要がある。

3） 従業員による理解

従業員のサイバーリスクに対する認識と理解が不足していることである。従業員は，自分の行動の潜在的な結果を十分に認識していない場合や，機密情報を保護するためのベストプラクティスを理解していない場合がある。人間はフィッシング攻撃などのソーシャルエンジニアリング攻撃の影響を受けやすいため，サイバーセキュリティにおいて最も脆弱な部分となる可能性がある。さらに，従業員がサイバーリスクに対する認識と理解を欠くことで，潜在的な脅威に効果的に対応することが困難となる。また，従業員などの内部関係者が脅威となるインサイダー脅威の問題も多く発生している。それは，システムやデータへのアクセスを許可されているにもかかわらず，個人的な利益や悪意によってその権限が悪用される状況である。例えば，2013年に米国政府の機密情報を漏洩した元国家安全保障局（NSA）請負業者であるエドワード・スノーデンのケースでは，機密情報に合法的にアクセスし，それを危険に晒したことで国家安全保障に対する重大なリスクを招いた。

4） 予算の制約

セキュリティ対策の実装に利用できるリソースは限られている。企業は主に予算の制約に直面することが多く，堅牢なサイバーセキュリティ・ソリューションに投資するために必要なリソースを十分に確保できない場合がある。そのため，包括的なリスク軽減戦略の導入が困難になる場合がある。さらに，サイバーリスクに伴う財務的影響を正確に評価することが困難な場合があり，サイバーリスク管理への投資を正当化することが困難となっている。そのため，NIST（米国立標準技術研究所）や業界団体などによって策定されたサイバーリスク管理フレームワークを組織全体のリスク管理戦略と統合することによって，サイバーリスク管理への構造化されたアプローチを実現し，予算・ミッションの重要性・リスク選好度などを効果的に評価することができる。サイバーセキュリティリスク管理のフレームワークにはいくつかの種類があり，広く一般的に用いられているフレームワークとしては，NIST による NIST Cybersecurity Framework（NIST CSF）がある。NIST CSF はサイバーリスク管理のベストプラクティスをまとめたフレームワークであり，10 のコントロールカテゴリーと 30 のコントロールで構成されている。また，ゴードンらによるサイバーリスク管理フレームワークでは，情報セキュリティに関するリスク監査，保険適用範囲の評価，利用可能な保険の評価，適切な保険を選択するための 4 ステップを提案している（Gordon, Loeb and Sohail〔2003〕）。このフレームワークではサイバーリスクを評価し，セキュリティ対策のギャップを特定し，保険適用に関して十分な情報に基づいた意思決定を行うための体系的なアプローチを提供する。

5） 優先事項のバランス

ビジネス目標との間で，厳格なセキュリティ対策を実装すると，システムの使いやすさや効率に影響が生じ，生産性が低下する可能性がある。さらに，サイバーセキュリティへの取り組みに十分なリソースと予算を割り当てることに組織内で抵抗がある可能性があり，効果的なリスク管理が妨げられる可能性もある。

6） 熟練したサイバーセキュリティ専門家の不足

サイバーセキュリティは，ネットワークセキュリティ，暗号化，マルウェア検出など，さまざまな技術ドメインの専門知識を必要とする複雑な分野である。企業はサイバーリスクを効果的に管理できる熟練したサイバーセキュリティ専門家を見つけて維持するのに苦労しており，需要が供給を上回り続けている。このことは，単に業界全体における人材不足だけでなく，小規模な組織では専任のサイバーセキュリティ担当者を雇用することが困難なまでに費用が高騰しているという状況も含んでいる。

7） コンプライアンスとガバナンス

サイバーセキュリティの実践と共に，遵守すべき法規制や業界標準への準拠を確認する必要がある。これには，ポリシーと手順の開発，監査の実施，コンプライアンス要件を満たすためのセキュリティ管理の実装が含まれる。

これらの課題や限界によってサイバーリスク管理戦略の効果的な実施が妨げられ，組織がサイバー攻

撃に対して脆弱になる可能性がある。そのため，これらの課題改善には，問題点を正確に把握することが必要である。企業は，サイバーリスク管理を優先し，潜在的な脅威を軽減するために必要なリソースを割り当てると同時に，教育およびトレーニングプログラムへの積極的な投資によって，企業はサイバーリスクに対する従業員の理解を向上させ，組織全体の意識を高めることができる。また，組織内での円滑なコミュニケーションによる協力体制を構築することで，リスク管理の取り組みを強化することができる。

残念ながら，継続的な改善に取り組んだとしても，これらの取り組みは常に完璧ではなく，企業はサイバー攻撃の被害を受ける可能性がある。しかし，企業がサイバーリスク管理プロセスを継続的に改善し，適切な対策を講じることによって，サイバー攻撃による被害を最小限に抑えることができる。企業がサイバーリスク管理プロセスによってリスクを最小限に抑えることができれば，経済的な損失を最小限に限定できる。また，企業が適切な対策を講じることで，サイバー攻撃による個人情報の漏洩やサービス停止などの被害を回避できる。さらに，企業がサイバーリスク管理プロセスを改善することで顧客や取引先からの信頼を高め，企業イメージを向上させることができる。

サイバーリスク管理プロセスの課題と限界を克服するために，企業が行う取り組みの一例について見てみる。1つの方法は，コラボレーションである。企業は他の企業や政府機関と協力して，サイバーリスクを管理することができる。例えば，企業は他の企業と情報共有することでサイバー攻撃の情報を共有し，攻撃を防ぐことに努めている。また，企業は政府機関と協力してサイバー攻撃の脅威を評価し，対策を講じることができる。インフラ事業者などの各業界に設置されたISAC（Information Sharing and Analysis Center）と呼ばれる組織では，業界での情報共有や分析が行われており，金融ISACや電力ISACといった組織が日本をはじめ各国に存在している。

もう1つの方法は，統合である。企業はサイバーセキュリティの機能を統合することで，リスク管理プロセスを効率化できる。例えば，企業は以下に掲げたようなサイバーセキュリティのツールやシステム，サイバーセキュリティ担当者の統合とコラボレーションによって，リスクをより効果的に管理できる。

- 他の企業と協力してサイバーセキュリティのトレーニングを実施
- 他の企業と協力してサイバーセキュリティの専門家を雇用
- 他の企業と協力してサイバーセキュリティのツールやシステムを開発
- 政府機関と協力してサイバーセキュリティの研究開発を実施

ここまでに述べた課題と限界を克服し，組織はサイバーリスクをより効果的に管理し，サイバー攻撃の被害を軽減することができる。

4. まとめ

本稿では，冒頭において，日本企業のサイバーリスク管理が立ち遅れている背景に①「過去にサイバー攻撃を受けたことがない」「サイバー攻撃を受けるような組織ではない」，②「サイバーセキュリティは技術的な問題である」，③「リスクマネジメントに充てる余裕がない，他に優先すべきことがある」，④「既存のセキュリティ対策で十分である」という4つの誤った認識があり，立ち遅れの解決に

は⑤「教育をとおして従業員のサイバーリスクに関する理解を深め，意識を向上させること」，⑥「組織内の円滑なコミュニケーションによる協力体制の構築の両面で推進すること」が不可欠であることを問題提起した上で，以下の内容について議論した。

まず，企業経営におけるサイバーリスク管理の定義，種類，影響について整理し，サイバーセキュリティにおけるリスクマネジメントプロセスの構造化に必要な要素を検討した。このリスクマネジメントプロセスで生じる課題と限界について，米国の先進事例や現時点でのベストプラクティスをもとに考察を行うとともに，サイバーセキュリティにおけるリスクマネジメントのフレームワークの構成要素を提示した。

次に，情報技術の進歩とデジタル化の進展に伴い，企業や個人が直面するサイバーリスクが複雑化・多様化している現状をふまえて，サイバーリスク管理の在り方について整理した。サイバーリスク管理とは，サイバー空間における脅威から資産を保護するために企業や組織が導入する戦略とプロセスであり，エンタープライズ・リスク管理フレームワークに統合することで，サイバーリスク管理の実践をビジネス目標に合わせて調整して，サイバーリスクを総合的かつ包括的に管理できるようになることを指摘した。サイバーリスク管理とサイバーセキュリティの向上において，企業が戦略的・戦術的・運用的アプローチにより，サイバーリスク対応を計画的かつ効果的に実施することで，消費者からの信頼や収益機会も高め，企業の信頼性と完全性の維持，法規制の遵守，組織の持続的成長を達成できるようになり，サイバーセキュリティのレジリエンスが構築されていくという考え方を提示した。これと併せて人的要因も重要な役割を果たすことに注目し，従業員教育や意識向上だけでなく，組織内における円滑なコミュニケーションとさまざまな部門間の調整とコラボレーションがリスク管理の要諦であるとした。そしてリスク管理のプロセスを整理して，「リスク識別」⇒「リスク分析」⇒「リスク対応」⇒「リスクモニタリング」⇒「リスクコミュニケーションと報告」の５つのステップで構成されるモデルを提示した。サイバーリスク管理プロセスの５つのステップを戦略的・戦術的・運用的なアプローチの一部として実施し，予算や人員を含む経営資源の割り当てにより具現化する道筋を明らかにした。これは，JIS Q 27001: 2014（ISO/IEC 27001: 2013）の「4. 組織の状況」「5. リーダーシップ」「6. 計画」「7. 支援」「8. 運用」「9. パフォーマンス評価」「10. 改善」に則してモデルを構築するために，セキュリティマネジメントフローを構造化したものである。

続いて，サイバーリスク管理プロセスの課題と限界をサイバーリスク管理のプロセスに即して，「脅威の急速な進化」「システムの複雑性と相互接続」「従業員による理解」「予算の制約」「優先事項のバランス」「熟練したサイバーセキュリティ専門家の不足」「コンプライアンスとガバナンス」という７つの要素について考察した。JIS Q 27001: 2014（ISO/IEC 27001: 2013）の「7. 支援」「8. 運用」で定められている項目が直面する課題を今日的に整理し，「9. パフォーマンス評価」「10. 改善」で特に注力すべき施策を検討したものである。そして結論として「人材の教育・トレーニング」「組織内の円滑なコミュニケーション」「他の企業や政府機関等とのコラボレーション」によるリスク管理の有効性について指摘した。

18 世紀以降の米国における企業経営の歴史を俯瞰すると，個人の専門化した事業と相互の繋がりからスタートした経済活動が，19 世紀後半から 20 世紀前半にかけて大企業をはじめとする組織と組織人の経済活動が大きな影響力を発揮するようになり，規模の経済や統合の経済が追求された。この過程で 20 世紀後半までに企業経営のマネジメント手法の研究と実践が蓄積され，さらに企業の社会的経済的責任への関心の高まりに応えるため，企業ガバナンスの制度整備が逐次行われるようになった。そして

21 世紀の第 4 次産業革命と言われる時代となり，経済の情報化・デジタル化が社会全体に広がったことを受け，サイバーリスク管理を含めた企業経営において，あらためて「人材」と「組織内ネットワーク化」「企業間および政府機関とのコラボレーション化」が，ガバナンスとマネジメントのキーコンセプトとなっていると言えよう。

サイバーセキュリティ・ベンチャーズの推計によると，2021 年の世界のサイバー攻撃総被害額は 6 兆ドル（約 660 兆円）と 2015 年の 3 兆ドルから倍増し，2027 年には 10 兆 5000 億ドル（1154 兆円）に拡大するとしている(4)。サイバー攻撃によるセキュリティ侵害の件数が増加する中で，企業は技術力に優れたサイバーリスク管理の人材が不足し，企業におけるサイバーリスク管理に必要なポストの人材を配置できず，サイバーリスクの脅威への対策が十分でない状況にある。セキュリティ侵害の発生頻度の増加やコストの増大，IT 人材の不足がサイバーリスクに直結しており，企業経営において高スキルな人材がサイバーリスク管理の要であることはいまや共通認識となっている。またガバナンスとしては，取締役会などトップマネジメントや企業幹部がサイバーリスク管理を重要視するとともに，サイバーリスク管理の知識とスキルの証明として求められる認定資格が重視され，安全保障の観点からもセキュリティクリアランスが重要となっている。その一方でスキルギャップ解消に役立つ人材を確保することはとても困難であり，すべての企業がサイバーリスク管理の高スキル人材を社内雇用によって解決することは困難なのが実情である。

JIS Q 27001: 2014（ISO/IEC 27001: 2013）に示された ISMS では，トップマネジメントのリーダーシップとコミットメントについて，「情報セキュリティ方針及び情報セキュリティ目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする」「組織のプロセスへの ISMS 要求事項の統合を確実にする」等，8 つの事項によって実証することが求められている。推進にあたっては，「組織の目的に対して適切である」「情報セキュリティ目的を含むか，又は情報セキュリティ目的の設定のための枠組みを示す」等，7 つの事項を満たす情報セキュリティ方針を確立しなければならない。そして，企業は ISMS が定められた状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。さらにトップマネジメントは，企業の ISMS が，引き続き，適切，妥当かつ有効であることを確実にするために，あらかじめ定めた間隔で，ISMS に関する外部及び内部の課題の変化や情報セキュリティパフォーマンスに関するフィードバック，利害関係者からのフィードバック，リスクアセスメントの結果及びリスク対応計画の状況等をレビューし，マネジメントレビューからのアプトプットには継続的改善の機会や ISMS のあらゆる変更の必要性に関する決定を含めなければならないとされている。このような PDCA サイクルを回すにあたり，トップマネジメントがリーダーシップを発揮して ISMS の適切性，妥当性及び有効性の継続的改善を推進することが，企業の責任として求められている。以上のように，サイバーセキュリティとマネジメントの統合的推進において，トップマネジメントや経営幹部が果たさなければならない役割はますます重要になっており，時間の経過とともに変化する外部及び内部の状況に迅速かつ的確に対応した組織戦略決定こそが，持続的経営を可能にすると言っても過言ではない。本稿でも考察したように，JIS Q 27001: 2014（ISO/IEC 27001: 2013）に示された ISMS の目指すべき姿と，個社のニーズ及び目的，セキュリティ要求事項，個社が用いているプロセス，並びに個社の規模及び構造等との間をつなぐ戦略的なサイバーリスク管理手法の必要性がさらに高まっている。

また情報化・デジタル化による事業環境と社会生活の変化に伴って巧妙化・高度化するサイバー攻撃の脅威は，従来のようなアンチウイルス等による事前防御だけでは不十分なことは企業経営者や取締役

会メンバーなどのトップマネジメントにとっても常識となってきているが，事前防御策をすり抜ける脅威をエンドポイント上で検知して対処するなど，サプライチェーンやバリューチェーン全体の防御やダメージコントロールについては，多くの企業にとっていまだ十分とは言えない状況にある。RaaS（サービスとしてのランサムウェア）の増加や，ダークウェブを通じたサービスとしての攻撃，CaaS（サービスとしての犯罪）を使ったビジネス的なサイバー攻撃等が今後さらに大きな脅威になると考えられている。またLLMや生成AIなどの機械学習による自動化，メタバース，Web3，エッジコンピューティングや量子コンピューティングなど最新のテクノロジー環境への対応に十分な経営資源を割り当てられる企業はまだ少ない。ビジネスプロセスやサービスを中断させる可能性があるインシデントを予測・予防，検出，対応，復旧し事業を再開する能力であるデジタルレジリエンスの強化は，企業価値の維持・発展に直結する経営課題である。さらに企業内だけでなく社会全体でのIoT活用が進む中，IoT資産の把握やリスク評価，リスク削減ポリシーの適用，既知の脅威の阻止，未知の脅威の検知・対応等も重要なテーマとなっており，日本でも2023年2月に国土交通省が運営する河川防災情報である簡易型河川監視カメラへの不正アクセス事案が発生したことは記憶に新しい(5)。

日本でもこのような全体状況を政府は政策課題として捉えており，金融庁の企業会計審議会（会長：徳賀芳弘京都先端科学大学副学長兼京都大学名誉教授）は，2023年4月7日に開催した総会で「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）」を取りまとめ公表した。主な改訂内容を見ると，まず内部統制の基本的枠組みとして「リスクの評価と対応」「情報と伝達」「ITへの対応」における重要事項が追加されている。「リスクの評価と対応」では不正に関するリスクについて考慮すること，「情報と伝達」では大量の情報を扱う場合はシステムが有効に機能することが重要であること，「ITへの対応」ではITの委託業務に係る統制，情報システムに係るセキュリティの確保が重要であることが追加されている。特にITに関する統制においては，ITの業務委託が担う範囲が重要となっていることや，サイバーセキュリティや情報漏洩によるインシデントが増加していることが背景になっている。

次に財務報告に係る内部統制の評価及び報告に関するものとして，ITを利用した内部統制の評価について，例えば，1年に1度評価を実施する，といったように特定の期間を定めて機械的に評価するのではなく，昨今加速するIT環境の変化を踏まえて評価すべき，という内容が追加されている。IT統制の対応では「情報システムの開発・運用・保守などITに関する業務を外部の専門会社に委託する場合」と「クラウドやリモートアクセス等の様々な技術を活用するに当たっては，サイバーリスクの高まり等を踏まえ，情報システムに係るセキュリティの確保が重要である」ことが追加されている。

米国ではGAFAM等のビッグテックだけでなく，ChatGPTを提供するOpenAI等も積極的にホワイトハウスや議会，政府機関と密接なコミュニケーションを取り，サイバーリスク管理の制度設計に大きな影響を与えている。彼らはルールメイキングの領域を視野に入れたコラボレーションを展開しており，現在公開されている情報を見ると，生成AI対策などサイバーリスク管理の今後の考察に不可欠の要素が盛り込まれている。このような先進的な事例や有効なプラクティスを，「人材の教育・トレーニング」「組織内の円滑なコミュニケーション」「他の企業や政府機関等とのコラボレーション」の3つの観点から詳細に分析し，現行施策の限界と解決すべき課題の洗い出しを進め，サイバーリスク管理のプロセスを定式化しつつ，戦略的・戦術的・運用的なアプローチの在り方を検討する。またサイバーリスク管理に十分な経営資源を割り当てられない小規模企業や非営利組織等が，サプライチェーンやバリューチェーンの脆弱性としてサイバー攻撃のターゲットになっていることも重要な課題である。そし

てサイバーリスク管理プロセスにおけるコミュニケーションの重要性と施策の統合手法に着目しながら，サイバーリスク管理を組織の中に取り込むことによってサイバーリスクを経営戦略に転化する経営管理について考察していく。サイバーリスク管理に関する考察の展望として示しつつ，今後の研究課題としたい。

［文責：第1節　辻（智），第2～3節　足立，第4節　辻（俊）］

《注》

（1） 前稿では，サイバーリスク管理を戦略的意思決定に取り入れるための方法について考え，経営戦略とリスクマネジメントの関係について新たな視点を提示した。詳細は辻他［2022］を参照。

（2） 中小企業のサイバーリスクに関しては Alahmari and Duncan［2020］を参照。

（3） サイバー攻撃の事例は世界中で枚挙にいとまがない。2021年の例で見ると，オーストラリアの大手クレーンメーカーの工場稼働停止やイギリスの通信事業者のサービス停止・障害など，多くの国や地域で被害が報告されている（独立行政法人情報処理推進機構（IPA）編［2022］164-167頁）。

（4） Morgan［2020］を参照。

（5） 国土交通省［2022］を参照。

（6） 金融庁企業会計審議会［2023］を参照。

参考文献

〈日本語文献〉

金融庁企業会計審議会［2023］「『財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）』の公表について」「コメントの概要及びコメントに対する考え方」「財務報告に係る内部統制の評価及び監査の基準（抄）新旧対照表」（https://www.fsa.go.jp/news/r4/sonota/20230407/20230407.html#bessi3）。

国土交通省［2022］「報道発表資料配信を停止している簡易型河川監視カメラの再開について」（https://www.fsa.go.jp/news/r4/sonota/20230407/20230407.html#bessi3）。

辻智佐子，足立嘉照，辻俊一［2022］「サイバーリスク管理の効率化と戦略的意思決定のための一考察」城西大学経営学研究科『The Josai Journal of Business Administration』第18号，2022年9月，1-19頁。

独立行政法人情報処理推進機構（IPA）編［2022］『情報セキュリティ白書 2022』実教出版。

〈英語文献〉

Alahmari, A., and Duncan, B., 'Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence,' *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (Conference Paper), June 2020.

Gonzalez-Granadillo, Gustavo et al., 'Automated Cyber and Privacy Risk Management Toolkit,' *MDPI Journals Sensors*, Vol. 21, Issue 16, August 15, 2021 (https://www.mdpi.com/1424-8220/21/16/5493).

Gordon, L. A., Loeb, M. P. and Sohail, T., 'A framework for using insurance for cyber-risk management,' *Communications of the ACM*, Vol. 46, Issue 3, March 2003, pp. 81-85 (https://dl.acm.org/doi/abs/10.1145/636772.636774).

Hooper, V. and McKissack, J., 'The Emerging Role of the CISO,' *Business Horizons*, Vol. 59, Issue 6, November-December 2016, pp. 585-591.

Kejwang, B., 'Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature,' *International Journal of Research in Business and Social Science*, Vol. 11, No. 6, September 12, 2022 (https://www.ssbfnet.com/ojs/index.php/ijrbs/article/view/1947).

Nan, Sun, et al., 'How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond,' *IEEE Access*, Vol. 10, January 1, 2022 (https://ieeexplore.ieee.org/

document/9810315).

Rosa, F. D., Maunero, N., Prinetto, P., Talentino, F., & Trussoni, M., 'ThreMA: Ontology-Based Automated Threat Modeling for ICT Infrastructures,' *IEEE Access*, Vol. 10, January 1, 2022 (https://ieeexplore.ieee.org/document/9936611).

Morgan, S., 'Cybercrime World $10.5 Trillion Annually By 2025,' *Cybercrime Magazine*, November 13, 2022 (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/).

To Integrate or Collaborate:
Strategies for Effective Cyber Risk Management and Cybersecurity

Chisako TSUJI・Shunichi TSUJI・Teruyoshi ADACHI

Abstract

In the current global and digital interconnected business environment, companies must adopt an offensive management approach to sustain growth while incorporating effective and efficient cybersecurity and cyber risk management into their business strategy. In this article, We pointed out the following points as a method for that purpose.

The cyber risk management process consists of five steps: risk identification, risk analysis, risk response, risk monitoring, and risk communication and reporting. Collaboration between employee education and organisational communication is critical. However, current cyber risk management faces challenges and limitations such as the rapid evolution of threats, increasing complexity and interconnectedness of systems, employee understanding, budget constraints, balancing priorities, shortage of skilled cybersecurity professionals, and achieving compliance and governance. Effective and efficient risk management requires cooperation with other companies and government agencies.

Keywords: Cyber risk management, Cyber risk assessment, Cybersecurity culture, Sustainable growth, Business continuity