なぜ企業にサイバーセキュリティ戦略が必要なのか
― サイバーリスクマネジメントに経営の意思を吹き込む ―

2026 年 3 月

本レポートの要点

― なぜ企業にサイバーセキュリティ戦略が必要なのか ―

企業を取り巻くサイバーリスクは、ランサムウェアによる事業停止、サプライチェーン全体に及ぶ障害、クラウド依存の増大、DX 推進に伴う統制の複雑化、攻撃対象範囲の拡大など、多面的かつ深刻な形で拡大している。こうした脅威の構造変化は、従来の技術対策中心のアプローチだけでは十分に対応できず、**経営としての意思と一貫した方向性を備えた「戦略」が不可欠である**ことを、近年の事例は強く示している。

本レポートは、国内外の最新動向と具体的な被害事例を踏まえつつ、サイバーリスクを経営リスクとして再定義し、**企業が中長期的に取り組むべき戦略の構造を体系的に整理したものである。**既存のガイドラインを包含しつつ、企業の実務に即した視点で再構成しており、経営者の意思決定に資する形で整理している点に特徴がある。

企業環境とリスク構造の変化

本レポートでは、国内統計、行政機関の報告、国際的な調査など複数の信頼できる情報源を参照しながら、企業が直面するリスクの特徴を立体的に捉えている。ランサムウェア被害の長期化、外部サービスを介した侵入、委託先で発生した問題の連鎖など、複数のレイヤーで同時にリスクが波及する現実は、もはや単一部門での対処が困難であることを示している。

企業は技術的対策の徹底に加えて、「侵入を前提とした備え」を構築し、事業継続やステークホルダー対応を含む広い視野での対策も必要であり、本レポートの分析もその点を重視している。

戦略としてサイバーセキュリティに取り組む意義

今日の企業は、**経営の判断基準そのものにサイバーリスクを組み込む**必要がある。本レポートでは、経営が戦略として取り組むべき理由を、以下のような視点から整理している。

- 守るべき価値やリスク許容度、優先順位を明確化し根拠ある形で定めることができるのは経営者である。
- 経営戦略・ERM・BCM・DX と整合した形で、サイバーセキュリティをガバナンス体制に統合するのは経営者の役割である。
- 組織文化への浸透、投資判断の妥当性、部門横断の連携を強化するのは経営者の意思と関与である。

本レポートでは、こうした課題に対し、単なる概念論ではなく **実務に落とし込み可能な枠組み**を提示している。

戦略構築と運用に向けた実践的アプローチ

戦略を構築し、組織に根付かせるためのステップについても、本レポートでは具体的に提示している。

- **状況分析・診断（As-Is 分析） → あるべき姿（To-Be）の定義 → ギャップ分析と課題整理 → 基本方針・重点施策 → 推進体制と制度設計 → 実行計画の策定**という一連のプロセスを整理し、企業が自社の規模・成熟度に応じて活用できるよう設計している。

- 既存の ISMS や事業継続計画（BCP）などの取り組みをベースに不足している要素を補完し、戦略として再構成・統合する考え方を示し、現場の余分な負荷を増やさずに全体最適化できる方法を提示。
- 経営層と現場を結び、戦略推進の中核を担う専門人材として「サイバーリスクマネージャ」の役割と能力を明確化。
- 外部アセスメントや演習などを通じて、戦略を継続的に更新していく仕組みを併せて整理。

これらは、企業が実際に「使える戦略」を構築するうえでの有益な土台となる。

サイバーリスクは、事業継続、企業価値、ステークホルダーからの信頼に直結する経営課題である。こうした状況において、企業が持続的に成長し、社会的信用を維持するためには、**経営者主導で明確な戦略を策定し、これを全社で運用する仕組みが不可欠**である。

本レポートの目的は、**サイバーリスクを経営リスクとして位置付け、経営者のリーダーシップのもとで戦略的にサイバーセキュリティを推進するための実践的指針を提示**することである。サイバー空間の脅威には技術的対策だけでは不十分である。**経営者の理解と関与のもと、ERM や BCM などのガバナンス視点を統合しながら、自社のあるべき姿に向けて継続的に取り組む**必要がある。そのための「道しるべ」として戦略を示すことの有効性を考察する。

＜各章の概要＞

第 1 章：サイバーリスクの脅威とリスクマネジメントの必要性

近年の事例をもとに、サイバー攻撃が企業活動に及ぼす影響を構造的に整理し、脅威の本質とリスクの深刻さを明確化する。“漠然とした不安”を、経営として認識すべきリスクへと具体化し、対応の出発点を提示する。

第 2 章：サイバーセキュリティ戦略の意義とその構造

なぜ個別対策の積み上げだけでは不十分なのか。その理由を経営視点から整理し、戦略として取り組む意義を示す。サイバーリスクを経営判断に統合するための構造（基本方針・重点施策・実行計画）を体系的に提示する。

第 3 章：サイバーセキュリティ戦略の策定－経営の意思を吹き込む

現状把握からあるべき姿の定義、ギャップ分析、施策化までの検討プロセスを整理し、戦略に経営の意思を反映する方法を示す。“どこから手をつけるべきか分からない”という課題を、実務的なステップに落とし込み、検討の軸と優先順位を明確にする。

第 4 章：サイバーセキュリティ戦略の実践と課題

策定した戦略を日常業務として運用するために必要な、経営のメッセージ、組織文化、人材、体制のあり方を整理する。戦略が形骸化しないための実務上のポイントを示し、組織全体で継続的に取り組むための基盤づくりを論じる。

第 5 章：まとめ

サイバーリスクを経営リスクとして一貫した方針のもとで管理することが、企業価値の維持と事業継続の基盤となることを総括する。

JCIC
Japan Cybersecurity Innovation Committee

なぜ企業にサイバーセキュリティ戦略が必要なのか

－ サイバーリスクマネジメントに経営の意思を吹き込む －

目次

はじめに

企業を取り巻く外部環境は一段と不確実性を増している。ロシアによるウクライナ侵攻に伴うエネルギー・食料価格の高騰、世界的なインフレ、米国の政策転換や地政学的緊張の高まりは、国際的なパワーバランスと経済情勢を大きく揺り動かしている。加えて、急激なテクノロジーの進化や人権・環境規制の強化、さらには一部で見られる反 DEI の動きなど、価値観の対立も顕在化し、企業経営の不確実性は一層高まっている。

このような複雑かつ不確実性の高い環境下では、企業は自社の経営計画やビジョンの達成を阻害し、事業継続に重大な影響を及ぼす可能性のある「重大リスク」を特定し、適切な対策を講じる全社的リスクマネジメント（ERM）が求められている[1]。

なかでも**サイバーリスク**は、ランサムウェアによる事業停止、サプライチェーンの混乱、情報窃取など、企業の事業継続を直撃する重大リスクとして再認識されている。サイバー攻撃は高度化・巧妙化が進み、一度の事故が事業継続や企業価値に深刻な影響を及ぼす事例は後を絶たない。さらに DX 進展に伴うシステムの高度化、クラウド化、外部サービス連携、サプライチェーン全体のデジタル化は効率化をもたらす一方、新たな脆弱性を生み出し攻撃対象領域を拡大している。

こうした背景から、サイバーリスクは、もはや情報セキュリティや技術部門だけで対処できる範囲を超え、企業価値の維持、事業継続、レピュテーションの保全といった経営の核心に直結する、**経営者が対処すべきリスク**となっている。企業は最悪の事態も起こり得る前提に立ち、経営者が主体的に関与する ERM の枠組みの中でサイバーリスクを位置付ける必要がある。加えて、重大な事業停止につながり得る点を踏まえれば、事業継続マネジメント（BCM）との連動も不可欠である[2]。

しかし多くの企業では、議論の出発点が攻撃手法や防御ソリューションといった技術的論点に偏り、経営として本来扱うべき全社的リスクマネジメントや事業継続の観点も含めた全体感の議論が不足しているのではないかといった懸念がある。本来、各企業は自社の事業にどのようなサイバーリスクが存在し、事業停止が社会へどのような影響を及ぼすか、何を守るべきか、サイバーセキュリティと事業継続のあるべき姿をどう描くかを経営者が議論し、中長期的な戦略として整理し全社的に推進すべきである。

本レポートの目的は、サイバーリスクを経営リスクとして位置付け、経営者のリーダーシップのもとで戦略的にサイバーセキュリティを推進するための実践的指針を提示することである。サイバー空間の脅威には技術的対策だけでは不十分である。経営者の理解と関与のもと、ERM や BCM などのガバナンス視点を統合しながら、自社のあるべき姿に向けて継続的に取り組む必要がある。そのための「道しるべ」として戦略を示すことの有効性を考察する。

---

[1] ERM（Enterprise Risk Management）：全社的リスクマネジメントとは、組織が価値を創造し、維持し、実現する過程においてリスクを管理するために依拠する、戦略策定ならびに実行と一体化したカルチャー、能力および実務である。出典「COSO 全社的リスクマネジメント　戦略およびパフォーマンスとの統合」（一般社団法人日本内部監査協会・八田進二・橋本尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会 COSO-ERM 研究会訳、同文舘出版、2018 年）

[2] BCM（Business Continuity Management）：BCP 策定や維持・更新、事業継続を実現するための予算・資源の確保、事前対策の実施、取組を浸透させるための教育・訓練の実施、点検、継続的な改善などを行う平常時からのマネジメント活動。出典　内閣府「事業継続ガイドライン」
https://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline202303.pdf

1. サイバーリスクの脅威－リスクマネジメントの必要性

本章では、近年の事例からサイバーリスクの脅威を概観し、その特徴と企業への影響、DX 進展によるリスク構造の変化を整理する。これらを踏まえ、経営としてリスクマネジメントを強化すべき理由を明確にする。

1.1 直近の事例からの学び

2025 年は、大手酒類・飲料グループや大手通販企業をはじめ、多くの企業がランサムウェア攻撃によって事業停止を余儀なくされた。これらの事案により、社会全体でサイバーリスクの影響がいかに甚大であるかを、あらためて強く認識する一年となった。

警察庁サイバー警察局の報告によれば、2025 年上半期のランサムウェア被害報告件数は 116 件に達し、過去最多水準にある。感染経路は VPN やリモートデスクトップ用の機器からの侵入が全体の 8 割以上を占め、その原因としては、ID・パスワード等が非常に安易であったことや、不必要なアカウントが適切に管理されずに存在していたことなどが指摘されている[3]。また、個人情報保護委員会の監視・監督報告では、民間事業者に対する指導案件のうち、不正アクセスが原因の個人情報漏洩事案が上半期 113 件（内、ランサムウェア攻撃 43 件）発生している。不正アクセスの主な原因は、ソフトウェアの脆弱性、ID・パスワードの脆弱性、アクセス制御の設定ミスが挙げられている[4]。

これらの原因は従来から広く認識され、注意喚起も継続されてきた。それでも直近の事例で依然として主な原因に位置づけられること自体が、対策を組織内部の隅々まで徹底し続けることの困難さを如実に示している。

こうした状況を踏まえ、企業は侵入を許す脆弱性への対応の徹底に加えて、万が一の事態を前提とした備えを強化する必要がある。特に直近で大きな被害に直面した企業の経営者は、今後のサイバーセキュリティへの取り組みとして概ね次の点を挙げている。

- **リスクマネジメントの高度化・強化**
- **全社ガバナンスの視点で俯瞰**
- **セキュリティ対策の最新化**
- **事業継続計画の見直し・強化**

私たちは、これらの事例から学び、社会全体としてサイバーセキュリティの向上に取り組んでいく必要がある。

表 1 ：2025 年上半期のサイバー被害に関する主要数値と原因

報告先	被害件数	原因等
ランサムウェア被害（警察庁）	被害報告件数：116 件	侵入経路：VPN・リモートデスクトップ経由が 8 割以上 原因：ID・パスワードが安易/不要アカウント管理不備
不正アクセスによる個人情報漏洩（個人情報保護委員会）	漏洩事案件数：113 件 うちランサムウェア起因：43 件	原因：脆弱性/ID・パスワード脆弱/アクセス制御設定ミス ※民間事業者の指導案件より

[3] 警察庁　サイバー空間をめぐる脅威の情勢等　https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

[4] 個人情報保護委員会　監視・監督の活動状況　https://www.ppc.go.jp/personalinfo/activity/　。2025 年上半期件数は令和 6 年度第 4 四半期と令和 7 年度第 1 四半期の合算値。

1.2 サイバーリスクの特徴と企業への影響

(1) 社会的影響と個社認識の乖離

社会全体を俯瞰すると、サイバー攻撃によるサービス停止、情報窃取、サプライチェーンを経由した二次被害などのインシデントは頻発しており、影響度が大きく、発生確率（頻度）も高いリスクとして認識されている[5]。一方で、個社レベルでは一定の対策が講じられているため、日常的に多くの攻撃が重大な被害に至る前に防御されている。そのため、自社では必要な対策済みとの認識から、深刻な被害が発生する確率は低～中程度と受け止められやすい[6]。

またサイバー攻撃は、物理的な事故のような視覚的インパクトに乏しく、経営者がニュース等で他社被害を知ったとしても、実際、その企業の内部でどのような事態が起きているかを実感として把握することは容易ではない。重大な事業停止を実際に経験した経営者は限られており、被害について詳細に語るケースもこれまでは多くなかった。このため、自社の対策水準が妥当かどうか判断する材料が不足し、結果として戦略的意思決定が後手に回るリスクが生じていた。この**「社会全体では深刻だが、自社では実感しづらい」**という構造的なギャップは、サイバーリスク特有の特徴のひとつである。

(2) 意図を持つ攻撃者の存在と攻撃手法の多様化

サイバーリスクは、設備故障や自然災害とは異なり、意図を持つ攻撃者が存在する点に根本的な特徴がある。攻撃者は、情報システムを構成するソフトウェアや機器の脆弱性、その管理不備、さらにフィッシングメールでユーザーの錯誤につけ込むなど多様な手法を用いて攻撃を行う。

その目的も金銭的利益、情報窃取、業務妨害、政治的主張、国家レベルの諜報活動、さらには愉快犯的動機や自己顕示まで幅広く、攻撃者の背景・動機・能力は一様ではない。こうした多様性に加え、攻撃手法は新たなツールや脆弱性の公開、闇市場での攻撃コード流通などにより日々高度化し、巧妙化している。

さらに、近年の攻撃者の特徴として、長期間にわたり企業内のネットワークに潜伏し、巧みに内部偵察や侵害範囲を広げながら攻撃機会をうかがう粘着性の高い攻撃が増えている。こうした継続的な侵害活動は、一般的なウイルス対策や社内ネットワークとインターネットの境界にファイアウォール等を設置する境界防御に依存した従来型の仕組みでは検知が難しく、発見の遅れが重大な事業停止や情報窃取へ直結するリスクを高めていることを、経営者は認識しておく必要がある。

このような、攻撃者による意図的・複雑・継続的な攻撃の性質を踏まえると、企業はサイバーリスクを、設備故障や自然災害のように発生確率で評価できる自然発生的なリスクではなく、**“狙われる前提”や“システムが停止する前提”で対応すべきリスク**として捉える必要がある。

---

[5] トレンドマイクロ株式会社の調査によると 2025 年 1 月～12 月に公表されたセキュリティインシデントは 559 件で、1 日当たり 1.5 件の発表ペースであった。出典：「2025 年の国内セキュリティインシデントを振り返る」、https://www.trendmicro.com/ja_jp/jp-security/25/l/securitytrend-20251211-01.html 。

[6] 英国拠点の専門保険事業会社 Beazley の Risk & Resilience レポートによれば、米国のビジネスエグゼクティブのうち「自社はサイバー脅威に対抗する準備ができている」と考える割合が前年より上昇しており、こうした自信が“false sense of security（誤った安心感）”につながり得ると指摘されている。出典：Risk & Insurance “U.S. Execs Show Overconfidence in Cyber Preparedness Despite Rising Threat Awareness” June 30, 2025、https://riskandinsurance.com/u-s-execs-show-overconfidence-in-cyber-preparedness-despite-rising-threat-awareness-survey/

(3) サイバー攻撃被害のサプライチェーンへの波及

サイバー攻撃による被害は、企業内部にとどまらない。情報システムや情報資産が侵害されると、その影響は自社を起点として、顧客、取引先や外部委託先、業務提携パートナーなどサプライチェーン全体に広がる可能性がある。現代の企業活動は、インターネットを介したデータ連携など高度に相互依存した構造の上に成り立っており、連鎖的に複数の企業に被害が発生するリスクが高まっている。

逆に、自社が依存する外部サービスやインフラ事業者において障害や侵害が発生した場合にも、自社の業務が被害を受ける可能性がある。自社の管理が及ばないサプライチェーンのどこか一つの領域で生じたシステム停止や機能不全が、自社の基幹業務の中断やサービス提供の遅延など重大な影響となって現れる事例が増加している[7]。

このように、サイバー攻撃は自社のみならずサプライチェーン全体に連鎖的な影響を及ぼす構造を持つため、企業は自社内の対策だけではなく、**業務委託先や外部サービスを含む広範な領域を視野に入れたリスク管理**が不可欠となっている[8]。

(4) サイバー攻撃被害の長期化と企業活動への深刻な影響

もし、自社の重要システムが 2 か月間停止するとどうなるだろうか。

売上、顧客対応、サプライチェーン、社会的信用――どこまで持ちこたえられるかを想像すると、その影響は決して小さくないはずである。

サイバー攻撃、とりわけランサムウェアによる基幹業務システムの暗号化は、企業の事業停止に直結する。さらに、サイバー攻撃からの復旧は、通常のシステム障害と比べて長期間を要する。その理由は、通常のシステム障害と異なり単なる機器交換やサービス再起動にとどまらず、攻撃者によって何をされたのか、潜伏していないのかなど**安全性を検証しながら段階的に業務を再開するという、多段階の復旧プロセスを必ず踏む必要**があるためである。復旧プロセスの全体像例は、表 2 のとおりである。

さらに、バックアップ自体が暗号化・削除（無効化）・破損・改ざんされている事例も多く、単純な復旧作業では対応できない[9]。また、侵入経路や侵害範囲を特定できない場合、どのシステムが安全か判断できず、ネットワークを遮断したまま再開の可否を慎重に検証する必要がある。さらには、システムを再構築するための環境をあらたに調達し、最初から構築し直す場合もある。

その結果、復旧には**数週間から数か月**を要することも珍しくなく、その間、**通常業務の継続は大きく制約**される。**こうした長期化は、売上機会の損失、追加コストの発生、顧客や取引先への影響、さらにはネット上での関心も呼ぶこととなり企業の社会的信用の低下**など、経営全体に広範な影響をもたらす。

---

[7] 経済産業省は、IPA を通じて実施した中小企業等におけるサイバーセキュリティ対策の実態調査結果として、過去 3 年間にサイバー攻撃の被害に遭った中小企業のうち約 7 割で取引先にも影響が及ぶ「サイバードミノ」が起きている実態を公表している。出典：経済産業省「中小企業の実態判明 サイバー攻撃の 7 割は取引先へも影響」（2025 年 2 月 19 日）https://www.meti.go.jp/press/2024/02/20250219001/20250219001.html

[8] サイバー攻撃の過失割合の指針については、JCIC「サイバー攻撃での過失割合に指針を」（2025 年 5 月 , https://www.j-cic.com/pdf/report/Degree-of-Negligence-in-Cyber-Attacks.pdf ）を参照されたい。

[9] 警察庁の「令和 7 年上半期におけるサイバー空間をめぐる脅威の情勢等について」によると、ランサムウェア被害 53 件のうち 51 件はバックアップを取得していたものの、そのうち 35 件ではバックアップ自体も暗号化されていた。
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf#page=70

表 2：サイバー攻撃発生時の復旧プロセス例

主要工程	内容
原因究明と証跡保全（フォレンジック）	侵入経路・侵害範囲を特定し、証拠の保全・分析を実施し、再侵入防止の根拠を明確化する必要がある。
封じ込め・除去・再発防止	社内ネットワーク内をラテラルムーブメント（横移動）で生じた痕跡を特定し、悪意のあるコード・不正設定・侵害アカウントを網羅的に除去し、構成・権限を再設計する。
データの整合性・完全性検証	バックアップが暗号化・削除（無効化）・破損・改ざんされていないかを確認し、復元後のデータ整合性を検証する。
認証基盤の健全化	資格情報の再発行、秘密鍵・証明書のローテーション、特権の棚卸と再付与を行う。
業務再開の安全性評価	段階的なネットワーク再接続、セグメンテーションの見直し、重要システムからの段階的再開とモニタリング強化を行う。
法令・契約対応	法的報告、規制当局・顧客・取引先への通知、契約上の義務履行を並行して進める。

1.3 DX 推進とリスク増大の不都合な関係

近年、企業におけるデジタルトランスフォーメーション（DX）は、競争力強化や業務効率化、新たな価値創出に向けて加速している。一方で、デジタル化の進展はサイバーリスクの構造を大きく変化させている。DX 推進がどのようにリスク増大につながっているかを三つの観点から整理する。

(1) デジタル技術活用の拡大による防御範囲の拡大

業務プロセスのデジタル化、クラウドサービスの活用、外部 API 連携、IoT デバイスやロボティクスの導入、生成 AI や AI エージェントの活用などにより、企業はサービス提供と業務オペレーションの利便性、柔軟性、効率性を大幅に向上させている。しかし、これらの技術が相互に連携することで、防御すべき範囲（アタックサーフェス）が急速に拡大し、自社が管理すべき領域と外部サービスやデバイス提供者が担う責任範囲が複雑に入り組む構造が生まれている。利便性・柔軟性・効率性の向上と引き換えに、**構成管理や統制の漏れが新たな脆弱性につながるリスク**が高まっている。

(2) サプライチェーンのデジタル依存の進展

企業は外部ベンダーや委託先との業務連携においてデジタル基盤への依存を強めており、サプライチェーン全体が複数のシステムやサービスによって成り立っている。このため、サプライチェーン上の脆弱性がそのまま自社のリスクへと波及する可能性が高まっている。攻撃者は相対的に防御が弱い企業を足がかりに主要企業へ侵入する手法を常態化させており、**サプライチェーンのどこかに脆弱性が存在すれば、自社の事業継続やオペレーションの安定性に直接影響するリスク**が高まっている。

(3) 急速なリモートワーク導入の影響と境界防御の限界

新型コロナウイルス対応として多くの企業が急速にリモートワークへ移行した際、短期間で構築されたネットワーク設定や暫定的な接続環境がそのまま運用に取り込まれ、脆弱な状態が残存していると指摘されている。国内外の調査でも、リモート接続用 VPN の設定不備や旧式プロトコルの利用、十分に保護されていない端末や家庭内ネットワークの継続利用などが、現在も攻撃対象になり続けていることが報告されている[10]。

現在は出社中心の勤務形態へ回帰する動きも見られるが、コロナ禍で拡大した VPN やリモートデスクトップなどのアクセス経路やデジタルデバイス利用の多様化は、引き続き企業ネットワークに組み込まれており、**従来の境界防御だけに依存したモデルではリスクを十分に把握・制御しきれない状況**が続いている。多様化したアクセス経路やデバイスを前提に、すべてを信用せず常に認証・検証するゼロトラストのセキュリティアプローチが求められている。

このように DX の進展は、企業に新たな価値をもたらす一方で、防御すべき範囲の拡大、外部依存の増大、境界防御モデルの限界といった構造的な変化により、サイバーリスクは質的にも量的にも増大している。企業は、常にセキュリティ対策を見直し最新の状態にする必要がある。

以上のことから、サイバー攻撃は事業停止、財務的負担、信用失墜など、企業活動全体に深刻な影響を及ぼす多面的なリスクと言える。これらの特性を踏まえると、**サイバーリスクを従来の技術的対策の枠内だけで管理することには限界があり、より広い経営視点から捉え直す**必要がある。

[10] Qollakaj, K. 他, “Cybersecurity of remote work migration,” Array, 2025. COVID-19 期の VPN 脆弱性と攻撃増加を分析。
https://www.diva-portal.org/smash/get/diva2:1988152/FULLTEXT01.pdf

Cybersecurity Insiders, “VPN Exposure Report 2025,” 2025. VPN の脆弱性と ZTNA 移行動向を示す調査。
https://www.cybersecurity-insiders.com/vpn-exposure-report-2025-why-organizations-are-adopting-a-modern-secure-access-strategy/

2. サイバーセキュリティ戦略の意義とその構造

本章では、サイバーセキュリティを経営戦略として位置づける意義を整理する。まず、経営者が担うべき役割と押さえるべき主要なポイントを明確にする。次に、戦略を構成する基本方針・重点施策・実行計画の構造を示し、企業が中長期的な視座でサイバーリスクに対応するための枠組みを整理する。

2.1 経営者の 3 つの役割と押さえるべき 5 つのポイント

ここまで述べてきたように、サイバー攻撃は情報セキュリティや技術部門だけで対処できる領域を超え、企業価値の維持、事業継続、レピュテーションの保全といった、経営の核心そのものに直結する問題となっている。攻撃の高度化と DX 依存領域の拡大により、一度のインシデントが企業活動全体を止め、社会的信用を大きく損ないかねない。

このような状況において必要なことは、経営者が「サイバーセキュリティは経営の責任である」という基本姿勢と方針を明確に示し、一段高い視座から組織全体を導くことである。経営者の役割と押さえるべきポイントを整理する。

(1) 経営者が果たすべき 3 つの役割

まず経営が果たすべき役割の第一は、**方針を定め明確に発信**することである。組織がどこに優先順位を置き、何を守るのかという基本的な方向性は、経営者が自らの言葉で示さなければならない。トップメッセージは単に形式的な宣言ではなく、従業員一人ひとりの行動を方向づけ、平時の規律や緊急時の判断に一貫性をもたらす企業文化の源泉である。サイバーリスクへの姿勢は、経営が発する言葉によって初めて組織の価値観として根付く。

第二に求められるのは、**投資判断における長期視点**である。サイバー攻撃による被害は、発生確率が読みにくい一方で、防御を突破されて一度発生すれば事業停止や顧客情報流出など極めて大きな影響をもたらす。したがって、短期的な費用対効果だけでは投資判断を行えない。サイバーセキュリティを“コスト”ではなく、“事業継続と企業価値を守るための必須投資”として位置づけ、長期的な資源配分を経営として決めていく姿勢が必要である[11]。

第三の役割は、**全社的な統合**である。サイバー攻撃がもたらす影響は、技術領域にとどまらず、法務、広報、サプライチェーン、BCP など多岐にわたる。重大インシデント発生時には、技術対処と同時に、取引先対応、行政報告、契約処理、企業としての説明責任など、経営判断の要素が数多く発生する。こうした状況に備えるためには、平時から指揮命令系統、役割分担、意思決定の基準を全社横断で統合しておく必要がある。

(2) 経営者として押さえるべき 5 つのポイント

これらの役割を実行可能な仕組みとして落とし込むために、経営として押さえるべきポイントが 5 つある。

第一に、サイバーセキュリティの位置づけを**戦略文書に明確に記載**し、守る対象やリスク許容度、復旧目標を経営の意思として言語化することである。第二に、ゼロトラストの導入や CSIRT 強化、バックアップ戦略の整備など、**継続的な投資を中期的なロードマップに組み込み、予算と人材を安定的に確保**することが求められる。第三に、**ガバナンスと責任分担を明確化**し、経営会議でサイバーリスクを定例的に扱う仕組みを整える必要がある。

---

[11] セキュリティ投資については、JCIC「社内のセキュリティリソースは『0.5%以上』を確保せよ」（2022 年 3 月，https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf）、JCJC「企業規模・業種別に見るセキュリティ投資・人員数の目安値」（2026 年 2 月、https://www.j-cic.com/pdf/report/Security-Investment-and-Staffing-Levels-by-Company-Size-and-Industry.pdf）を参照されたい。

さらに、**サイバーリスクを ERM や BCM と一体で扱い**、事業継続の観点から重要業務の優先度や代替手段を整理することが第四のポイントである。そして最後に、**レピュテーションと法規制対応を平時から前提に置き**、外部公表や顧客説明、行政連絡の判断基準をテンプレート化し、訓練しておくことが、重大インシデント時の信用回復を大きく左右する。

これらの取り組みを通じて、企業はサイバー危機に直面した際にも、経営としての整合性とスピードを確保できるようになる。サイバーセキュリティはもはや IT 部門の課題ではなく、企業の存続と信頼を守るための経営そのものである。経営者がこの認識を持ち、平時から備えることが、企業価値を守る最も重要な行動である。

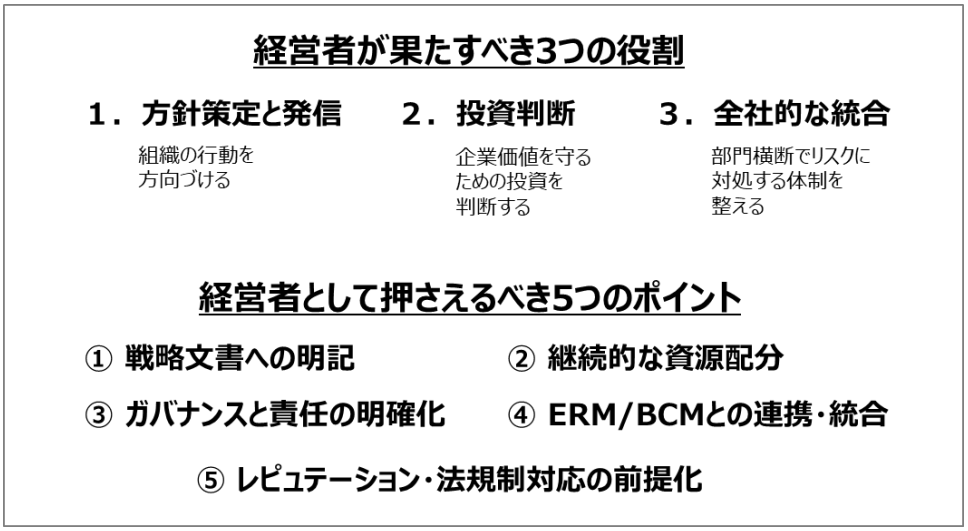

図１：サイバーリスクに対する経営者の役割と押さえるべきポイント

次節では、これらのポイントを具体的にどのように戦略に反映するかについて考察する。

2.2 企業経営におけるサイバーセキュリティ戦略の意義

企業経営における「戦略」とは、単なる計画や施策の羅列ではなく、企業が長期的に競争優位を確立し、持続的に価値を創出するための意思決定の枠組みである。戦略は、環境変化の中で企業が進むべき方向性と優先順位を定め、限られた資源をどこへ投下するかを判断する基盤となる。戦略が欠如すれば意思決定は場当たり的となり、組織全体の行動も一貫性を失う。逆に、明確な戦略は変化への適応性を高め、長期的な信頼の維持を支える拠り所となる。

戦略は“策定”にとどまらず“実行”されてこそ意味がある。

戦略研究の第一人者であるリチャード・P・ルメルトは、「**戦略とは、組織の存亡に関わる重大な課題や困難に対して立てられるものであり、それらと無関係に立てられた目標とは異なる。**」と述べ、優れた戦略の構造（戦略のカーネル（核））を次の三つで説明している[12]。

[12] Richard P. Rumelt, *Good Strategy/Bad Strategy: The Difference and Why It Matters*, Crown Business, 2011.
（邦訳：リチャード・P・ルメルト『良い戦略、悪い戦略』（村井章子訳、日本経済新聞出版、2012 年）

戦略のカーネル（核）

- **診断（Diagnosis）**：問題の本質の把握
- **基本方針（Guiding Policy）**：問題にどう対処するかの道しるべ
- **行動（Coherent Action）**：資源投入と行動の一貫性

本レポートでは、**サイバーリスクという"組織の存亡に関わる課題"に対し、状況を診断し、課題を明確化し、それに対処する基本方針・重点施策・実行計画を体系化したものを「サイバーセキュリティ戦略」**と位置づける。企業はこの戦略の下で全社的な意思統一を図り、適切に資源を投入し、中長期的に一貫した行動を可能にすることで、サイバー上の課題解決と事業の持続性の両立を目指すことができる。

2.3 戦略の要素と構造

本節では、サイバーセキュリティ戦略を構成する**基本方針、重点施策、実行計画**の要素の三層構造と相互関係を示し、企業が戦略を設計・運用する際の骨格を整理する。

(1) 基本方針：企業の方向性を定める最上位概念（WHY）

基本方針は、企業がサイバーリスクにどのような姿勢・価値観・方向性で臨むかを示す戦略の最上位レイヤーである。**経営者自身の考えを簡潔で分かりやすい言葉で示す**ことで足りるが、ここでは、基本方針をさらに**ビジョン／ミッション／目的・目標**の三つに分解して整理する例を紹介する。

① ビジョン（Vision）：企業が目指す将来像

ビジョンは、中長期におけるサイバーセキュリティの「あるべき姿」を示す。経営戦略と整合した将来の到達点であり、企業の判断基準となる。

例：

- サイバー脅威に強い事業基盤を確立し、社会から信頼される企業となる
- 安全なデータ活用を基盤に、DX を継続的に推進できる組織となる
- レジリエンスを備え、変化する脅威に迅速に適応できる企業となる

② ミッション（Mission）：ビジョン実現のための基本姿勢・原則

ミッションは、ビジョンを実現するために企業がどのような姿勢・原則で取り組むかを示すものであり、経営者と従業員の行動指針となる。

例：

- サイバーセキュリティを経営課題として位置づけ、継続的に改善する
- 全社員がリスクを理解し、自律的に行動できる文化を育む
- 外部専門家やガイドラインを取り入れ、最適な防御態勢を追求する

③ 目的・目標（Goals / Objectives）：対象ごとに達成したい成果を定義する

目的・目標は、ビジョン／ミッションを具体的な達成像に落とし込むものであり、事業領域、顧客／パートナー、社員などの対象ごとに定義するとよい。各目標は、KGI／KPI 等の定量指標とレビュー頻度を付与し、誰が・いつまでに・どの水準まで到達するかを明確にする。

例

- 対象：**事業（プラットフォーム／サービス）**：
  ビジネスエコシステムの基盤として、顧客・パートナーに対してセキュアなプラットフォームを提供する。
  指標例：重要サービスの停止率、重大脆弱性の残存率　等。
- 対象：**顧客・パートナー（信頼／品質）**：
  顧客・パートナーから安心して選ばれる経営品質を維持・向上する。
  指標例：第三者保証（例：SOC2/ISO）の維持、対外アシュアランスの提供率 等。
- 対象：**社員（働き方／行動変容）**：
  社員一人ひとりが情報資産を守り、様々な人と場で協働できるセキュアな環境を整備する。
  指標例：全社員研修受講率、フィッシング耐性指標の改善　等。

これらのビジョン、ミッション、目的・目標によって、戦略全体の方向付けと、組織が共有すべき価値観・成果基準を明確にする。

(2) 重点施策：基本方針を実現するための主要テーマ（WHAT）

重点施策は、基本方針を実現するために企業が強化すべき主要な領域である。技術対策にとどまらず、自社の課題に応じてガバナンス、人材、組織文化、サプライチェーンなど、企業のリスク構造に応じた広範な領域が含まれる。最近の企業の再発防止策事例などから重点施策として検討すべき項目を例示する。

重点施策として検討すべき項目例

- **ガバナンス強化**
- **技術的基盤の強化**
- **人材育成・組織文化の醸成**
- **サプライチェーンセキュリティ**
- **インシデント対応能力の強化**
- **情報共有（社内外の連携）**

詳細は次章で説明する。

(3) 実行計画：重点施策を進めるためのロードマップ（HOW）

実行計画は、重点施策を実際に進めるためのタスクにブレークダウンする。企業のリスク状況とリソースに応じて、短期・中期・長期の時間軸に加え、担当部門と期限を組み合わせて整理することで、責任主体と進捗管理が明確となる。なお、実際の計画策定の手法や形式は各社の運用に応じて柔軟に設定すればよく、重要なのは、優先順位と責

任が明確であり、経営として進捗を継続的に把握できるよう設計されていることである。表 3 は、重点施策をタスク／サブタスクとしてブレークダウンするイメージである。

表 3：重点施策ごとにタスクにブレークダウンするイメージ

重点施策	タスク／サブタスク	主担当／副担当部門	期限	……
① ガバナンス強化	①-1 経営者への定期報告プロセスの整備	経営企画部門／リスク管理部門、情報セキュリティ部門、CSIRT	○年○月	……
	①-2 ERM/BCM との連携・統合	リスク管理部門／事業継続管理部門／情報セキュリティ部門	○年○月	……
	①-3 ポリシー・標準・手順の整備	……	……	……
	①-4 役割・権限と責任の明確化	……	……	……
② 技術的基盤の強化	②-1 ゼロトラストアーキテクチャの導入	……	……	……
	②-2 ……	……	……	……
③ 人材育成・組織文化	③-1 ……	……	……	
④以下省略				

次節では、サイバーセキュリティ戦略の実装例を紹介する。

2.4 サイバーセキュリティ戦略の具体例

(1) 我が国のサイバーセキュリティ戦略

サイバーセキュリティ戦略の最も具体的で企業が理解し、参考とすべきものは、我が国のサイバーセキュリティ戦略である[13]。これは、「サイバーセキュリティ基本法」に基づき、おおむね 3 年ごとに策定される国家レベルの戦略文書である。最新版は 2025 年 12 月 23 日に閣議決定され、サイバー空間を巡る脅威の増大に対応し、官民一体で中長期的に取り組むべき方向性と施策を体系的に示している。

この戦略は、国家として今後 5 年間を見据えた脅威認識、基本原則、重点施策、推進体制を整理した包括的な枠組みであり、以下の 4 つの 章で構成される。

Ⅰ. 策定の趣旨・背景

Ⅱ. 本戦略における基本的な考え方

Ⅲ. 目的達成のための施策

Ⅳ. 本戦略の推進体制

[13] 国家サイバー統括室 「サイバーセキュリティ戦略」 https://www.cyber.go.jp/policy/jyuyo-bunsho/index.html

第Ⅰ章では、国家レベルでサイバーセキュリティ対策を一体的に推進するため、目標や実施方針を体系化し国内外に示す必要性が明記されている。第Ⅱ章では、基本原則（例：情報の自由な流通、法の支配、開放性、自律性、多様な主体の連携）や、国際情勢・脅威動向・デジタル化の進展を踏まえた情勢認識が提示されている。第Ⅲ章では、防御・抑止、人材・技術、社会全体のレジリエンスなど、国家として取り組むべき重点施策が整理されている。第Ⅳ章では、官民連携・国際協働を含む推進体制が示されている。

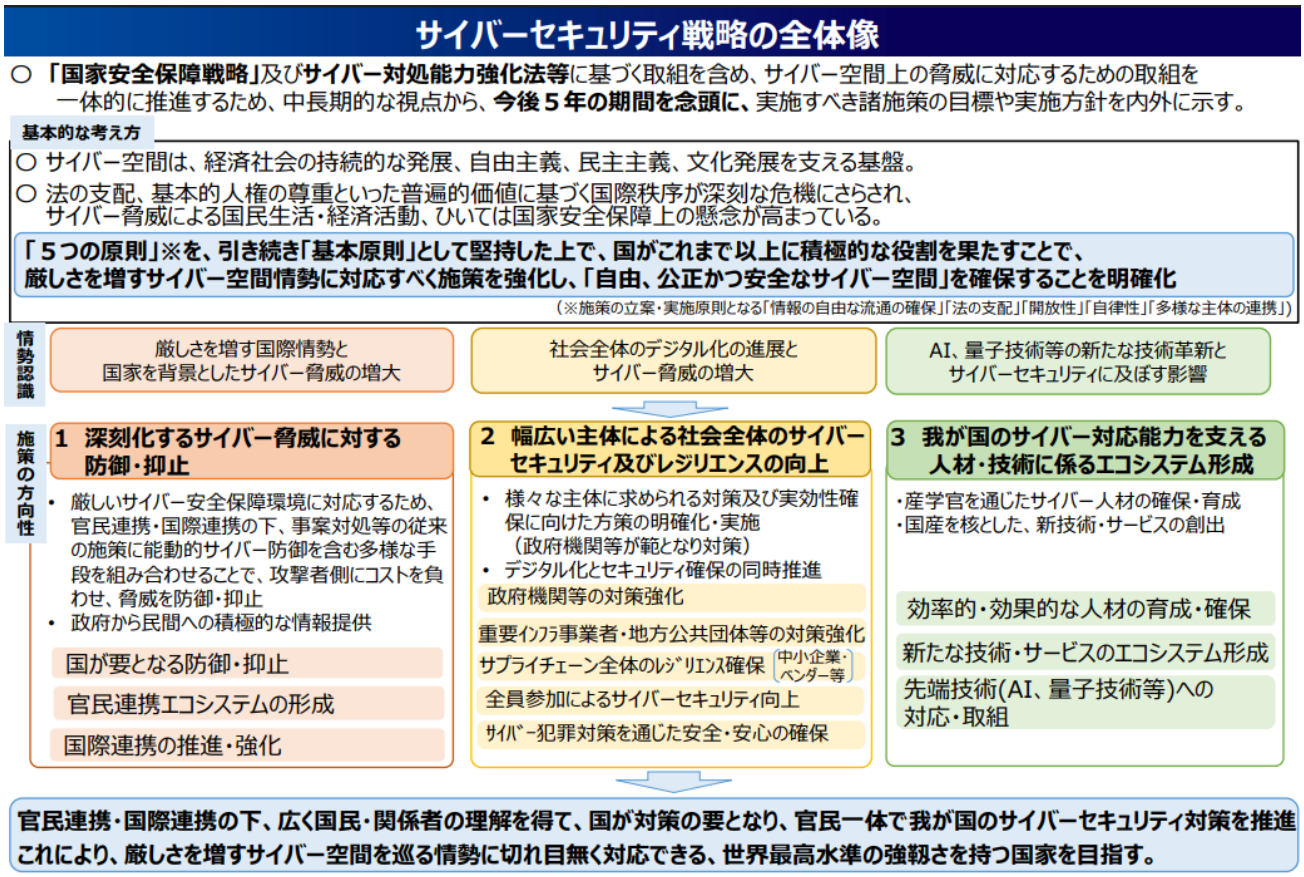

図２：我が国の「サイバーセキュリティ戦略」の全体像[14]

●企業が参考にすべきポイント

我が国のサイバーセキュリティ戦略は、国家レベルでの脅威認識と対応方針を体系化したものであり、企業にとっても次の観点で参考となる。

① 基本原則の明確化

国家戦略の冒頭で示される「確保すべきサイバー空間の在り方」や基本原則は、企業が自社として「何を守るのか」、「どうあるべきか」を定義する際の基盤となる。例えば、国家戦略が示す基本原則（情報の自由な流通／開放性／法の支配など）は、企業のセキュリティポリシーや行動指針の上位概念として応用できる。

[14] 出典：国家サイバー統括室 「サイバーセキュリティ戦略の概要」 https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025_abstract.pdf

② 情勢認識に基づく施策の方向性

国家戦略では、国際情勢、社会のデジタル化、AI・量子技術の影響などが情勢認識として整理されている。企業にとっても、外部環境の変化は脅威・リスクの前提条件である。下記動向を踏まえ、自社のリスク評価と施策設計に反映させる必要がある。

- ランサムウェアの高度化
- 生成 AI を悪用したフィッシング
- サプライチェーン攻撃の増加

③ 目的達成のための重点施策の整理

国家戦略では以下のような重点施策が掲げられている：

- 深刻化する脅威に対する防御・抑止（能動的サイバー防御を含む）
- 社会全体のレジリエンス強化（重要インフラ・地方公共団体・中小企業）
- 人材・技術エコシステムの形成

企業においても、「防御・復旧」、「人材育成」、「サプライチェーン管理」、「事業継続計画（BCP）」といった施策は戦略の核となる。国家戦略の体系は、施策群の整理方法として参考になる。

④ 推進体制の整備

国家戦略が官民連携・国際連携を重視し、推進体制を明示している点は、企業における

- 経営者の関与
- 部門横断の推進体制
- 社外との連携（委託先・業界団体・政府）

を構築する際に参考になる。特に国家戦略では、政府（NCO）が情報集約や分析を行い、官民連携エコシステムを整備する方針を明記しており、企業側もこれを踏まえた連携基盤の整備が求められる。

(2) 企業のサイバーセキュリティ戦略の例

企業がサイバーセキュリティ戦略を策定・運用するにあたっては、自社の事業特性やリスク環境、さらには顧客・パートナーとの関係性を踏まえた独自の戦略を構築する必要がある。実際、多くの企業においてサイバーセキュリティ戦略に相当する方針や施策が策定され運用されていると思われるが、それらを明確に「サイバーセキュリティ戦略」という呼称で開示しているケースは必ずしも多くない[15]。そこで本レポートでは、企業のサイバーセキュリティ戦略の一例として、筆者が所属する企業において 2018 年に策定し、現在も継続的に推進しているサイバーセキュリティ戦略を紹介する。

この戦略は、経営者の主導のもと、サイバーセキュリティに関するビジョン、ミッション、目的・目標を明確に定義し、これを実現するための重点施策を体系化したものである。この戦略では、企業グループ全体の情報セキュリティ基本方針のもとで、まず企業として目指すサイバーセキュリティの姿を短く明瞭な言葉で示し、経営者・従業員・グループ各社が共

[15] 直近 1 年間に提出された有価証券報告書の「事業の状況」を対象として、EDINET を使用し全文検索した結果の該当件数（社数）は次の通りであった。検索文字列が「情報セキュリティ」：2,213 件、「サイバーセキュリティ」：553 件、「サイバーセキュリティ戦略」：4 件。検索実施：2026 年 1 月 23 日。金融庁「EDINET について」：https://www.fsa.go.jp/search/20130917.html

通認識を持つための基本方針を設定している。そのうえで、CISO が主導するサイバーセキュリティ戦略推進体制により、重点施策をタスクレベルまで分解して実行に移す形態をとっている。戦略は内外環境変化を踏まえ毎年度見直すとともに、3 年ごとに NIST サイバーセキュリティフレームワーク（CSF）を用いたアセスメントを実施し、その結果をリスクベースで優先順位を付け、3 か年計画として反映している[16]。

表 4：企業のサイバーセキュリティ戦略の例

情報セキュリティ基本方針	（前略）情報セキュリティ対策をグループ役職員全員の意識に浸透させるとともに、サイバー攻撃など社会全体の課題に取り組みサプライチェーン全体で常に世界最高水準の情報セキュリティレベルを目指すことをここに宣言します。（中略）私たちは顧客・パートナーと共に社会を豊かにする価値を提供し、社会課題を解決する企業にふさわしいサイバーセキュリティ経営を実践します。（後略）

サイバーセキュリティ戦略

ビジョン：	多様な企業をつなぐビジネスエコシステム創出企業に成長するためにプロアクティブでセキュアな環境を提供する。			
ミッション：	顧客・パートナーと共に社会を豊かにする価値を提供し、社会課題を解決する企業にふさわしいサイバーセキュリティ経営・マネジメントを実現する。			
目的・目標：	1． ビジネスエコシステムの基盤として顧客・パートナーに対してセキュアなプラットフォームを提供する。 2． 顧客・パートナーから安心して選ばれるため、自社グループの経営品質を維持・向上する。 3． 社員一人ひとりが情報資産を守り、様々な人と場で協働できるセキュアな環境を整備する。			
重点施策：	1．システム関連施策 • 顧客システムおよび社内システムにおける技術的対策の強化 • DevOps セキュア環境の整備 • CSF など外部基準に準拠した継続的改善 • クラウドサービスの安全な利用 • 防御機能の企画・運営	2．組織・プロセス関連施策 • CSIRT 機構の強化 • 現場セキュリティ対応力強化 • クラウドサービス利用領域でのセキュリティ強化 • グループ会社全体のセキュリティガバナンス強化	3．人材関連施策 • クライシスマネジメントの強化（経営者/組織長/一般社員） • サイバーセキュリティ対応能力向上のための計画的施策 • サイバー演習の定期実施 • CSIRT 要員の強化・拡充	4．見せる化施策（情報開示・コミュニケーション） • 顧客・パートナー・サプライチェーンへの透明性の提供 • 社内外への情報発信（IR・統合報告書など） • バックキャスト型セキュリティマネジメント
戦略が準拠する外部の指針・基準・標準・ガイドライン等				
経団連「サイバーセキュリティ宣言 2.0」	経済産業省「サイバーセキュリティ経営ガイドライン」[17]	日本政府「サイバーセキュリティ戦略」	NIST サイバーセキュリティフレームワーク (CSF)、他	

（出所）筆者が所属する企業の事例を一部加筆修正し作成

[16] 米国立標準技術研究所 (National Institute of Standards and Technology)、「The NIST Cybersecurity Framework (CSF) 2.0」（February 26, 2024、https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf、邦訳：IPA「米国国立標準技術研究所 サイバーセキュリティフレームワーク（CSF） 2.0」（https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf)

[17] サイバーセキュリティ経営とは、経営者が自らのリーダーシップのもと、全社的にサイバーセキュリティ対策を推進する経営の在り方である。経済産業省と IPA が策定した『サイバーセキュリティ経営ガイドライン Ver.3.0』では、経営者が認識すべき「3 原則」と、CISO 等の責任者に指示すべき「重要 10 項目」を提示しており、これらを実践することが企業の持続的成長と競争力強化に不可欠であるとされている。

3. サイバーセキュリティ戦略の策定－経営の意思を吹き込む

本章では、企業が実効性あるサイバーセキュリティ戦略を構築するための基本ステップを整理する。さらに、既存の取り組みを戦略に統合する視点を提示し、企業が中長期的に持続可能な形でサイバーリスクへ対応するための検討に役立つ視点と枠組みを提供する。

3.1 戦略策定の基本 6 ステップ

サイバーセキュリティ戦略を、まったく初期の段階から策定する場合には、以下の 6 つのステップに沿って進めることが有効である。これらのステップは、現状の把握から、あるべき姿の定義、課題整理、戦略方針の設計、推進体制、実行計画の策定までを一貫して整理したものである。なお、自社の成熟度や事業特性に応じて、実施の範囲や深度を調整することが望ましい。

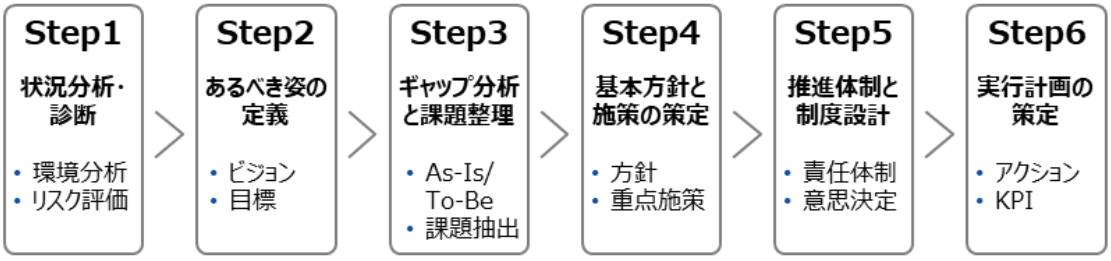

図 3：サイバーセキュリティ戦略策定の基本ステップ

戦略策定にあたっては、経営者のリーダーシップのもとで検討体制を組成することが重要である。特に、これまでに実施してきたリスクマネジメント、情報セキュリティマネジメント、事業継続マネジメントといった関連領域は、戦略策定の基盤として大きな価値を持つ。これらを統括する CxO（CISO、CRMO、CIO 等）や主要事業部門の責任者を中心にチームを編成することで、既存の知見と成果物を活用しつつ、網羅的かつ効率的に検討を進めることが可能となる。

Step1：状況分析・診断（As-Is 分析）

まず、自社を取り巻く環境を多面的に把握し、次の観点から現状を明確にする。

- 自社の事業停止や情報窃取が、自社・顧客・社会に与える影響
- 重要事業において想定されるサイバーリスク
- 現時点の対策状況とその限界、改善すべき領域

リスクアセスメント、事業影響度分析、脅威分析、過去のインシデント情報、各種方針や手順書などを活用して整理する[18]。

[18] 事業影響度分析については、内閣府「事業継続ガイドライン－あらゆる危機的事象を乗り越えるための戦略と対応－（令和５年３月）」 https://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline202303.pdf を参照されたい。

Step2：あるべき姿（To-Be）の定義

状況分析の結果を踏まえ、自社がサイバーリスクから何を守り、どのような姿を実現すべきかを定義する。To-Be を、成熟度の最高点やベストプラクティスの完全実装として置いてしまうと、現実との乖離が大きくなり、戦略が画餅となる。To-Be は、企業の事業特性とリスク許容度を踏まえ、経営上の要請（守るべき価値）から定義する。

- どの事業・情報資産をサイバーリスクから保護すべきか
- 目指すべき状態、どの程度の停止や情報漏えいが許容不能なのか
- 自社がサイバーセキュリティに取り組む意義は何か（ビジョン、ミッション）

これらは戦略の基準点となり、後続の施策策定・優先順位付けの根拠となる。

Step3：ギャップ分析と課題整理

現状（As-Is）とあるべき姿（To-Be）を比較し、その差分をギャップとして整理する。抽出した課題については、重要度・緊急度・影響度などの観点から優先順位を設定し、戦略が解くべきテーマを明確化する。Step1 から Step3 の検討に役立つ視点と枠組みについては次節で説明する。

Step4：基本方針と施策の策定

Step3 で整理した課題に基づき、戦略全体の方向性となる基本方針を定め言語化する。そのうえで、次の観点などから課題解決に必要な施策を体系化する。

① **ガバナンス強化**：統治構造、役割・責任、意思決定プロセス、グループ会社や委託先に対する統制など、組織横断で整合性を確保する。

- 経営者への定期報告プロセスの整備
- 全社的リスクマネジメント（ERM）/事業継続マネジメント（BCM）との連携・統合
- 政府が示す各種ガイドライン、セキュリティ対策評価制度、NIST CSF など国際的な評価基準の活用
- 役割・権限と責任の明確化、ポリシー・標準・手順の整備

② **技術的基盤の強化**：重要資産を起点とした予防・検知・復旧の強化、クラウド・ゼロトラストへの対応、ログ基盤や監視体制など、リスクと投資のバランスを踏まえて構築する。

- ゼロトラストアーキテクチャの導入
- 資産管理・脆弱性管理・ログ管理・バックアップファイル管理
- SOC／CSIRT 体制の強化[19]
- クラウド・SaaS の安全性確保

③ **人材育成・組織文化**：必要人材の確保と育成、属人化の解消、全社リテラシー向上、心理的安全性を伴う報告文化など、組織能力としてのセキュリティを高める。

[19] SOC：Security Operation Center、企業等のシステムやネットワークを 24 時間 365 日監視し、サイバー攻撃の検知・分析・対応を行う専門チーム。CSIRT：Computer Security Incident Response Team、企業等でサイバー攻撃や情報漏洩などのセキュリティインシデント発生時に、検知、分析、封じ込め、復旧、再発防止を行う専門チーム。

- 研修体系の構築（一般社員～管理職～専門家）
- 行動規範や組織文化レベルでの浸透
- セキュリティ人材の確保・育成・外部活用

④ **サプライチェーンセキュリティ**：委託先・取引先・クラウドサービスなど、外部依存に対する統制や契約管理、評価と是正プロセスを整備する。

- ベンダー評価と基準の設計
- 契約書へのセキュリティ要求組み込み
- 共同演習や情報共有の枠組み整備

⑤ **インシデント対応能力の強化**：初動の迅速化、危機管理体制の明確化、演習による意思決定の検証、復旧のレジリエンス強化。

- 年間計画による訓練・演習
- 初動手順の明確化・フォレンジック体制
- 危機管理広報との連携・法規制対応

⑥ **情報共有**：部門間連携、経営報告、法務・広報との連動、外部機関（ISAC、業界団体等）との協働を通じた知見活用。

- 社内外との連携強化

基本方針と重点施策は、単なる対策羅列ではなく、**戦略としてのストーリー**を持つ必要がある。すなわち、「なぜその施策が必要で、どの課題を解決し、どの価値を守るのか」を明確にしたうえで、実行可能性と優先度を考慮して体系化することが求められる。

Step5：推進体制と制度設計

策定した戦略を実効性のあるものとするため、責任体制と意思決定プロセスを設計する。特にサイバーセキュリティ戦略を確実に推進するための部門横断のプロジェクト体制を CISO のもとに設置するなどが有効である。

- 経営者・リスク管理部門・情報システム部門・主要事業部門などの役割と責任の明確化
- 組織横断で戦略を推進するための推進体制や会議体（例：サイバーセキュリティ戦略推進プロジェクト、リスク委員会、セキュリティ委員会）
- モニタリング手順や承認プロセス等の制度設計

これにより、戦略が日常的に運用される枠組みが整う。

Step6：実行計画の策定

Step5 で設置した推進体制が中心となり、策定した基本施策を、具体的なアクションに分解し、担当部門・期限・予算・KPI を設定する。短期・中期・長期の時間軸で整理し、優先順位とリスクに基づいて実現可能性を評価しながら、3ヵ年計画などの現実的なロードマップとしてまとめる（表 3 参照）。

3.2 既存の取り組みを活用し戦略に昇華

多くの企業はすでに何らかの形でサイバーセキュリティに取り組んでいる。社内の情報資産管理、ネットワーク運用、脆弱性対応、インシデント報告、社員教育、外部委託管理――これらは一見ばらばらに見えるが、実は企業のサイバーセキュリティ戦略を構成する一部として機能している。また、事業継続計画（BCP）も多くの企業で大規模地震などの災害を対象として策定されている。

本レポートでは、サイバーセキュリティ戦略を「ゼロから新しく作る」ものとして捉えるのではなく、**すでに存在するこれらの取り組みを土台にして、不足している要素を補完し、経営者が全体を体系化し連動することで、実践可能な戦略を構築する**という立場を採る。

このアプローチは各部門のこれまでの取り組みを活かしながら、現場負荷を増やさず、既存活動の価値を高め、企業全体の納得感を得られる現実的な方法である。

●サイバーセキュリティ戦略構築の考え方：

既存の取り組みを可視化し、欠けている要素を補完し、サイバーリスクへのリスクマネジメントの横串を通し、経営の意思を吹き込むことで、全体を一貫したストーリーと統治構造に再構成する

●この考え方の利点：

(1)現場負荷増加を最小化し、(2)既存活動を否定せずに納得感を得やすく、(3)実行可能性（実装力）が高い

3.3 検討に役立つ視点と枠組み

サイバーセキュリティ戦略を実効性のあるものにするためには、現状（As-Is）と目指す姿（To-Be）の差を明確にし、差分を施策・投資・体制・ルールへ落とし込む必要がある。特に経営者にとって重要なのは、サイバーセキュリティを「IT 部門の技術課題」としてではなく、**企業価値・事業継続・信頼に直結する経営課題**として把握し、意思決定できる状態にすることである。

この分析を行う際には、サイバーセキュリティに特化した NIST サイバーセキュリティフレームワーク（CSF）を活用する方法もある。しかし、初期段階から膨大な技術論に深く入りすぎると経営者の参画が難しくなるため、まずは組織全体を俯瞰できるフレームワークを用いて網羅性を確保することを推奨する。

この目的に対して有効な枠組みの一つが、マッキンゼーの 7S である[20]。7S は、戦略や組織といった“目に見えやすい要素”だけでなく、文化や価値観といった“見えにくい要素”も含めて全体を俯瞰できるため、サイバーセキュリティの実態を**「仕組み」「人」「統治」「文化」**の観点で一貫して評価できる。とりわけ、経営が関与すべき領域（ガバナンス、投資判断、リスク許容度、対外説明、企業文化）を整理して可視化できる点で、戦略策定の基盤として適している。

表 5 に、7S を用いたサイバーセキュリティのギャップ分析に使用するフレームワーク例を示す。なお、NIST CSF と 7S の対応関係は必要に応じて「付録 1 ：7S× CSF 2.0 マッピング表」を参照されたい。

[20] マッキンゼーの「7S モデル」では、Strategy（戦略）、Structure（構造）、Systems（制度）、Shared Values（価値観）、Skills（スキル）、Staff（人材）、Style（業務スタイル）の 7 つの要素を用いて組織を総合的に分析する。

表 5：サイバーセキュリティに対するギャップ分析に使用するフレームワーク例

要素	現状（As-Is）	あるべき姿（To-Be）	課題（ギャップ）	解決方針
1.戦略（Strategy）	自社の経営方針や経営ビジョンの達成を阻害するサイバーリスクへの対応方針や取り組み状況などの現状	左記に対するあるべき姿	ギャップを課題として列記する	課題に対する解決方針
2.組織構造（Structure）	サイバーセキュリティに対応する組織や体制の状況などの現状	〃	〃	〃
3.システム・制度（System）	サイバーセキュリティに対応する技術的・組織的・人的・物理的対策の状況などの現状	〃	〃	〃
4.人材（Staff）	高度なサイバーセキュリティに対応できる人材の確保・育成などの現状	〃	〃	〃
5.スキル・能力（Skill）	組織を構成する要員が保持すべきスキル・能力とその状況などの現状	〃	〃	〃
6.経営スタイル・社風（Style）	自社の経営スタイル・企業風土とサイバーセキュリティの相互作用などの現状	〃	〃	〃
7.共通の価値観（Shared Value）	サイバーセキュリティに対する価値観・理念の状況などの現状	〃	〃	〃

サイバー領域へ適用する際には、評価観点を「運用手順の点検」や「技術対策」に寄せ過ぎないことが重要である。経営者が判断に使える評価観点にするには、「何が整っているか」ではなく、「経営として統治できているか」「投資の妥当性を説明できるか」「企業価値の毀損を許容できるか」という問いとする。

経営者向けの評価観点を以下に示す。

●7S 要素に基づく As-Is/To-Be 分析の経営者向け評価観点

(1) 戦略（Strategy）：企業価値・成長戦略と整合しているか

サイバーリスク対応は、経営戦略・重点事業・中期計画と整合して初めて「戦略」と呼べる。ここで問うべきは、方針の有無だけではなく、**企業価値への影響を前提に優先順位と投資を決められる状態**になっているかである。具体的には、サイバー事故が起きた場合の財務影響、信用毀損などの影響を想定し、ERM（全社的リスク管理）やBCP/BCM（事業継続）と統合的に扱えているか、経営としてのリスク許容度（どこまでを許容し、どこからを許容しないのか）が明確か、といった点が評価の中心となる。戦略の観点が確立されることで、セキュリティ施策は「場当たり的な対策の積み上げ」ではなく、「守るべき最重要資産に資源を集中する設計」へ移行できる。

チェックポイント	• 経営としての守るべき最重要資産（事業・顧客・知財・稼働）と許容度を明確にしているか • サイバーリスクは、中期経営計画・成長戦略・重点事業の前提条件として織り込まれているか • 重大サイバー事象が起きた場合の財務影響（売上減少、コスト、賠償）と信用影響 を定量/定性で把握しているか • サイバーリスクを ERM（全社的リスク管理）のトップリスクとして位置づけ、定期的に経営レビューしているか • リスク低減だけでなく、顧客信頼・取引条件・競争力を高める戦略（差別化）として扱えているか

(2) 組織構造（Structure）：責任と意思決定が機能しているか

サイバーセキュリティは、部門横断調整を要する経営課題である。したがって、組織構造の評価では「担当部署があるか」だけではなく、**平時・有事ともに意思決定が滞りなく行える構造か**を問う必要がある。CISO 等の責任者の設置はもちろんのこと、経営への報告ライン、決裁権限、事業部門・IT・法務・リスク管理・広報など関係者が連携する会議体が実際に機能しているかが重要となる。さらに、重大インシデント時に、誰が停止判断を行い、誰が対外説明や当局対応を主導するのか、判断の権限とプロセスが事前に定義され演習で検証されているかが、統治の成熟度となる。

チェックポイント	• サイバーセキュリティ責任者（CISO 等）を設置し、その責任範囲が明確になっているか • 全社横断で推進するための委員会や会議体などのガバナンス体制を整備しているか • 海外拠点・グループ会社・委託先を含めた統制の及ぶ範囲のガバナンスを設計しているか • 危機発生時に、誰が何を決めるか（停止判断、対外説明、当局対応）を事前に決めているか

(3) システム・制度（System）：投資が「守るべき価値」に直結しているか

システム・制度の評価は、技術要素の多さから細部に入りやすい。しかし経営者向けの評価としては、細かな技術項目の網羅よりも、**投資が「守るべき価値（重要資産）」に対して適切に配分されているか**が本質となる。すなわち、予防・検知・復旧（レジリエンス）の要素が、最重要資産を中心に一貫して設計されているか、外部基準（NIST/ISO 等）に照らした成熟度を経営が理解できる形で把握し、改善ロードマップとして管理できているかが問われる。また、クラウドや外部委託、サプライチェーンを通じた第三者リスクについても、事業実態に即した統制（契約・評価・監査・是正）が整備され、形骸化していないことが重要である。ここが弱い場合、対策は分断し、コストをかけても経営としての安心に繋がらない。

チェックポイント	• 守るべき最重要資産に対して、必要十分な対策を取っているか • 確固たる外部セキュリティ基準（NIST CSF、ISO/IEC 27001 等）に照らした自社の成熟度を経営者が把握しているか • 「平時の効率」だけでなく、危機時のレジリエンス（迅速な復旧・継続）を実現できるシステム・制度になっているか • クラウド・委託先・サプライチェーンに対する統制が、事業実態に合わせて整備されているか

(4) 人材（Staff）：体制は事業責任を果たせる水準か

人材の観点では、単に人数が足りているかではなく、重大事故が起きたときに **事業継続・対外対応を含めて遂行できる体制か**が評価の軸となる。統治、監視、危機対応、法務連携、広報連携など必要機能が明確になっており、採用・育成・外部委託を含む確保策が現実的なのかが重要である。経営者が見るべきは、「担当者が頑張っているか」ではなく、**体制が継続可能で、再現性を持って機能する設計になっているか**である。

チェックポイント	• 現状の体制で、重大インシデント発生時に事業継続・対外対応まで遂行できるか • 必要な人材ポートフォリオ（統治、運用、監視、危機対応、法務連携等）が定義され、確保策（採用・育成・委託）があるか • 24 時間 365 日監視や緊急対応など、必要な稼働要件を満たす体制か（自社/委託の最適設計ができているか）

(5) スキル・能力（Skill）：組織能力として再現性があるか

スキルは個々人の研修や資格の話に矮小化しがちだが、経営の観点では、サイバー対応が**組織能力として再現可能**であるかが肝要である。経営・事業・IT それぞれに必要なスキル（危機時の意思決定、対外説明、リスク評価、初動対応など）が定義され、演習を通じて実効性があるかを確認する。特に、演習の結果が教訓として整理され、プロセスや体制、ルールの改善につながっているかは、実効性の指標となる。全社の基礎リテラシーが低い場合、フィッシング等の侵入口を塞げず、対策投資の効果が出にくくなるため、スキルのギャップは経営上のボトルネックとして扱うべきである。

チェックポイント	• 役割ごとの必要スキル（技術、リスク理解、マネジメント）を定義しているか • スキル習得のための研修体系（基礎・実務・高度・演習）を整備しているか • スキル評価の仕組み（資格、認定制度、研修履歴）を透明性をもって運用しているか • 現状スキルの棚卸し（可視化）を定期的に行っているか

(6) 経営スタイル・社風（Style）：経営の姿勢が現場に伝わっているか

Style は、経営者の関与が最も問われる領域である。経営者がサイバーリスクを「IT の問題」ではなく「信頼と継続を守る経営責任」として語り、投資判断や評価制度に反映させているかが、現場の行動を左右する。加えて、インシデン

トやヒヤリハットが隠蔽されず迅速に報告される心理的安全性が確保されているか、責任追及ではなく学習と改善を重視する文化が根づいているかが重要である。Style が弱い組織では、問題は表に出ず、初動が遅れ、被害が拡大する。一方で Style が成熟した組織では、早期報告と改善が回り、結果としてレジリエンスが高まる。

チェックポイント	• 経営者がセキュリティに対して明確なメッセージ、行動、投資判断を示しているか • セキュリティに関する基礎意識（フィッシング、情報管理等）が組織文化として浸透しているか • 心理的安全性とコミュニケーションが、インシデント報告や改善提案を促す風土になっているか • “責任追及型”ではなく“学習・改善型”の文化が根づいているか

(7) 共通の価値観（Shared Value）：理念としての信頼を守れているか

共通の価値観は、企業の理念・行動規範とサイバーセキュリティの整合性を問う。顧客・社会の信頼を守るという価値観が、単なるスローガンではなく、製品・サービス設計、取引、投資判断、事故時の対外説明方針に反映されているかが評価の中心となる。ここが明確であれば、現場は迷ったときに判断基準を持つことができる。逆に価値観が曖昧であれば、短期の効率や都合が優先され、結果として信頼毀損のリスクが高まる。サイバーセキュリティを「信頼を資産として守る経営活動」と位置づけられるかどうかは、共通の価値観の成熟度に左右される。

チェックポイント	• 自社がサイバーセキュリティに取り組む意義は何か（ビジョン、ミッション） • 組織のミッション・バリューに、セキュリティに関する価値観が明確に位置付けているか • 組織内でその価値観が共有され、日常の行動規範に落とし込まれているか • ステークホルダー（顧客、取引先、社会）への責任としてセキュリティを捉えているか • 価値観が施策や投資判断に反映される仕組み（方針、会議体、評価）があるか

4. サイバーセキュリティ戦略の実践と課題

本章では、策定したサイバーセキュリティ戦略を企業内で実践し、継続的に運用していくうえでの主要な課題と取り組むべき要点を整理する。

4.1 経営トップによるサイバーセキュリティ経営宣言の重要性

サイバーセキュリティを企業経営の中核に据えるためには、経営トップによる明確なコミットメントが不可欠である。経営者が自らの言葉でサイバーセキュリティの重要性を社内外に発信することは、組織全体の意識を高め、文化として定着させるうえで極めて重要な意味を持つ。特に、経営トップの承認と支援を明示することで、サイバーセキュリティ戦略の優先順位と実効性を高め、部門間調整や投資判断において「経営者の意思決定に基づく戦略」として組織内の合意形成を容易にする。宣言の主な意義は以下の通り。

- 社内へのメッセージ：サイバーセキュリティが経営課題であることを明確にし、全社員の行動変容を促す。
- 社外へのメッセージ：顧客、取引先、株主、規制当局などに対して、企業としての責任ある姿勢を示す。
- 戦略の正当性の担保：経営者の承認と支援を明示することで、戦略の実行力と優先順位を高める。

宣言すべき内容については、一般社団法人 日本経済団体連合会（以降、経団連）の「経団連サイバーセキュリティ経営宣言 2.0」を参考とすることを推奨する[21]。これは、経済界が全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献すべく、1.経営課題としての認識、2.経営方針の策定と意思表明、3. 社内外体制の構築・対策の実施、4. 対策を講じた製品・システムやサービスの社会への普及、5. 安心・安全なエコシステムの構築への貢献という 5 つの事項の実践に努めることを宣言したものである。

宣言を周知する形式としては、社内イントラネットでの公開、社外向け Web サイトでの掲載、統合報告書やサステナビリティレポートへの記載などが考えられる。

宣言を一過性のものにしないためには、以下のような仕組みと連動させることが重要である：

- 戦略との整合性：宣言内容が戦略のビジョンや施策と一貫していること
- モニタリングと報告：戦略の進捗状況を経営者が定期的に把握・評価する仕組み
- 経営者の継続的関与：委員会への参加、定例報告の受領、外部発信の継続など

経営トップによるサイバーセキュリティ経営の宣言は、戦略の実効性を高めるとともに、企業の信頼性と持続可能性を支える基盤となる。経営者の言葉と行動が一致していることが、組織全体の信頼と行動変容を促す鍵となる。

4.2 サイバーセキュリティ意識醸成の必要性

攻撃者側は常に組織やサービスの隙を狙っており、守る側は新たな技術やデバイスの普及によって防御すべき領域が拡大し続けている。企業としてセキュリティのためのルールや仕組みを整備し、技術的対策を講じていても、時間の経過

[21] 経団連サイバーセキュリティ経営宣言 2.0 https://www.keidanren.or.jp/policy/2022/087.html

とともにどこかに隙が生まれ、完全な防御は困難である。どのような大きな事故であっても、実際は些細なことがきっかけで発生することが多い。それぞれを分析すると、わずかな気の緩みや意識の低下が真因として挙げられる。サイバーセキュリティも例外ではない。どれほど堅牢な仕組みを構築しても、人間が関与する部分がある限り、組織を構成する誰か一人の油断が外部からの侵入を許す原因となり得る。サイバーセキュリティを強化するためには、社員一人ひとりがその基礎となる意識を持つことが不可欠である。**一人ひとりの社員がサイバーセキュリティを自分ゴトとして捉える**ことが、非常に重要な課題である。これらの取り組みについては、関連する JCJC レポートを参照されたい[22]。

4.3 戦略実践におけるサイバーリスクマネージャの役割

サイバーセキュリティ経営を実践するためには、戦略の策定と体制構築に加え、こうした運用基盤の整備と、それを担う人材の育成・活用が不可欠である。経営者と現場の間に立ち、戦略の実行状況を把握し、課題を抽出・整理したうえで、改善提案を行う。また、現場に対しては、方針の浸透、施策の支援、教育の推進などを担い、戦略の持続的な運用を支える**サイバーセキュリティ・リスクマネジメント領域におけるリスクマネージャ**が求められる（以下、サイバーリスクマネージャと呼称する）。

サイバーリスクマネージャは、自社が直面するサイバーリスクを正確に認識し、現実的な視点から最悪のシナリオまで想定した事前準備を推進する。リスクが顕在化した場合、どのような影響が連鎖し、どれほどのインパクトをもたらすのかを具体的に考え想定・評価することが重要である。そのうえで、リスク評価やポリシー策定にとどまらず、IT 部門や法務部門などの他部門と密接に連携し、経営者と現場をつなぐ「橋渡し役」として全社的なリスクマネジメント戦略を主導する役割を担う。

また、重大インシデント発生時には、迅速かつ的確な判断が不可欠である。サイバーリスクマネージャはリスク管理担当役員（CRMO）や情報セキュリティ担当役員（CISO）を補佐し、特にランサムウェアによる基幹システム停止といった緊急事態においては、CSIRT による初動対応の結果を踏まえて、組織全体での事業継続・復旧や社内外ステークホルダーへの情報発信、レピュテーションリスク対策までを主導することが求められる。

企業は、サイバーリスクマネージャとなる人材の育成・確保も必要である。（「付録２：サイバーセキュリティ・リスクマネジメント領域におけるリスクマネージャの主な役割」参照）

4.4 継続的な改善の必要性

サイバーセキュリティ戦略は、一度策定すれば終わりではなく、継続的に見直し、改善していくことが不可欠である。脅威環境や技術、法規制、ビジネスモデルの変化に対応するためには、戦略の実行状況を定期的に評価し、必要に応じて修正を加える仕組みが求められる。サイバーセキュリティを取り巻く環境は日々変化しており、セキュリティ対策は常に最新にする必要がある。静的な戦略では対応が困難である。

次のような変化に対応するため、戦略の定期的な見直しが必要となる。

---

[22] セキュリティ人材については、JCIC「攻めのプラス・セキュリティ人材で DX with Security の実現を」（2022 年 1 月、https://www.j-cic.com/pdf/report/Proactive-Plus-Security-Human-Resources.pdf ）、サイバーセキュリティの自分ゴト化については、JCJC「サイバーセキュリティを自分ゴト化する」（2025 年 8 月、https://www.j-cic.com/pdf/report/Making-Cybersecurity-Ones-Own.pdf）を参照されたい。

- 新たな脅威や攻撃手法の出現
- 法規制や業界ガイドラインの改定
- 組織構造やビジネスプロセスの変更
- セキュリティ技術の進化

このような変化に柔軟に対応するために、PDCA サイクルや **OODA ループ**を戦略運用に組み込むことが有効である[23]。また、NIST サイバーセキュリティフレームワーク 2.0 など確固とした基準やガイドラインに基づき、例えば 3 年ごとに外部の目を入れた定期的なアセスメントで成熟度を測ることも有効である。

[23] OODA ループは、Observe（観察）、Orient（状況判断）、Decide（意思決定）、Act（実行）の 4 要素を高速で繰り返し、変化の激しい環境で迅速に対応する意思決定フレームワーク。OODA ループの詳細についてはチェット・リチャーズ『OODA LOOP（ウーダループ）』（原田勉訳、東洋経済新報社、2019 年）を参照されたい。

5. まとめ

経営者が自らコミットして戦略策定に関与することで得られる主要な効果を、以下に整理する。

(1) 全社一体となった組織横断の取り組みが可能となる

サイバーセキュリティを企業戦略として位置づけることで、従来の「情報システム部門主導の個別対策」から脱却し、事業部門、管理部門、経営者が共通の目的と優先順位を共有できる。これにより、業務プロセスの見直し、委託先管理、訓練・演習、BCP 対応などを部門横断で統合的に進めることが可能となる。

(2) 中期的・計画的な資源配分・投資が可能となる

戦略として目指すべき方向性と投資原則が明確化されることで、アーキテクチャの更新、バックアップ高度化、SOC/CSIRT の強化、人材育成など、継続的で計画的な投資を中期計画に組み込めるようになる。これにより、単発のツール導入ではなく、企業全体の成熟度を段階的に高めるための組織的な資源配分が実現する。

(3) 意思決定の一貫性と迅速性が高まる（ERM との整合）

戦略に基づくリスク基準（守るべき資産、リスク許容度、優先順位など）を ERM に統合することで、投資判断、ロードマップ更新、委託先管理、例外承認といった日常の意思決定が、方針と整合した形で運用されるようになる。これにより、サイバーリスクが他の重要リスクと同じ基準で評価され、判断のばらつきが抑えられるとともに、意思決定のスピードも向上する。

(4) BCP 連携による事業継続能力（レジリエンス）の強化

サイバーリスク対応を事業継続計画（BCP）と連携させ、復旧手順、代替プロセス、暫定運用（機能縮退）、代替サイト、広報・顧客対応などを含む統合的な対応体制を整備することで、重大事態発生時でも事業を「維持・縮退・代替」で継続する能力が高まる。これにより、企業全体のレジリエンスが強化される。

(5) ステークホルダーからの信頼性と説明責任の向上

サイバーセキュリティを企業戦略として明示することで、リスク管理体制や意思決定プロセスを透明性のある形で外部に説明できるようになる。これにより、株主、取引先、規制当局、顧客など多様なステークホルダーとの信頼関係が強化され、調達条件や信用評価にも好影響を与える。

このように、サイバーセキュリティ戦略は、技術対策の集合を超え、企業全体の方向性、優先順位、資源配分、意思決定の基準を整えることで、組織のレジリエンスとガバナンスを根本から強化するものである。

本レポートが、各社の経営者が自社の事業とリスク構造に即したサイバーセキュリティ戦略を策定し、ERM や BCM と連携・統合した統治の仕組みとして運用していくための実践的な手がかりとなることを期待する。また、サプライチェーンを含む関係者との連携を通じ、社会全体としてのセキュリティ水準の底上げにつながることを願う。

以上

付録１：7S × NIST CSF 2.0 マッピング表

7S 要素	7 S 要素のチェックポイント例	CSF2.0 カテゴリ
1.戦略 （Strategy）	戦略・目的・リスク基準の設定 ・ 経営としての守るべき最重要資産（事業・顧客・知財・稼働）と許容度を明確にしているか ・ サイバーリスクは、中期経営計画・成長戦略・重点事業の前提条件として織り込まれているか ・ 重大サイバー事象が起きた場合の財務影響（売上減少、コスト、賠償）と信用影響 を定量/定性で把握しているか ・ サイバーリスクを ERM（全社的リスク管理）のトップリスクとして位置づけ、定期的に経営レビューしているか ・ リスク低減だけでなく、顧客信頼・取引条件・競争力を高める戦略（差別化）として扱えているか	・ 組織の状況（GV.OC） ・ リスクマネジメント戦略 GV.RM） ・ ポリシー（GV.PO） ・ 監督（GV.OV） ・ サイバーセキュリティサプライチェーンリスクマネジメント（GV.SC） ・ 資産管理（ID.AM） ・ リスクアセスメント（ID.RA）
2.組織構造 （Structure）	組織体制・ガバナンス・委員会 ・ サイバーセキュリティ責任者（CISO 等）を設置し、その責任範囲が明確にしているか ・ 全社横断で推進するための委員会や会議体などのガバナンス体制を整備しているか ・ 海外拠点・グループ会社・委託先を含めた統制の及ぶ範囲のガバナンスを設計しているか ・ 危機発生時に、誰が何を決めるか（停止判断、対外説明、当局対応）を事前に決めているか	・ 役割、責任、権限（GV.RR） ・ 改善（ID.IM） ・ インシデント復旧のコミュニケーション（RC.CO）
3.システム・制度 （System）	技術・プロセス・運用・制度の全体 ・ 守るべき最重要資産に対して、必要十分な対策を取っているか ・ 確固たる外部セキュリティ基準（NIST CSF、ISO/IEC 27001 等）に照らした自社の成熟度を経営者が把握しているか ・ 「平時の効率」だけでなく、危機時のレジリエンス（迅速な復旧・継続）を実現できるシステム・制度になっているか ・ クラウド・委託先・サプライチェーンに対する統制が、事業実態に合わせて整備されているか	・ アイデンティティ管理、認証、アクセス制御（PR.AA） ・ データセキュリティ（PR.DS） ・ プラットフォームセキュリティ（PR.PS） ・ 技術インフラのレジリエンス（PR.IR） ・ 継続的監視（DE.CM） ・ 有害事象の分析（DE.AE） ・ インシデント管理（RS.MA） ・ インシデント分析（RS.AN） ・ インシデント対応の報告とコミュニケーション（RS.CO） ・ インシデント軽減（RS.MI） ・ インシデント復旧計画の実行（RC.RP）

7S 要素	7S 要素のチェックポイント例	CSF2.0 カテゴリ
4.人材 （Staff）	人材確保・配置・役割分担 ・ 現状の体制で、重大インシデント発生時に事業継続・対外対応まで遂行できるか ・ 必要な人材ポートフォリオ（統治、運用、監視、危機対応、法務連携等）が定義され、確保策（採用・育成・委託）があるか ・ 24 時間 365 日監視や緊急対応など、必要な稼働要件を満たす体制か（自社/委託の最適設計ができているか）	・ 役割、責任、権限（GV.RR）
5.スキル・能力 （Skill）	技能・訓練・運用能力 ・ 役割ごとの必要スキル（技術、リスク理解、マネジメント）を定義しているか ・ スキル習得のための研修体系（基礎・実務・高度・演習）を整備しているか ・ スキル評価の仕組み（資格、認定制度、研修履歴）を透明性をもって運用しているか ・ 現状スキルの棚卸し（可視化）を定期的に行っているか	・ 意識向上とトレーニング（PR.AT）
6.経営スタイル・社風（Style）	経営姿勢・意思決定スタイル ・ 経営者がセキュリティに対して明確なメッセージ、行動、投資判断を示しているか ・ セキュリティに関する基礎意識（フィッシング、情報管理等）が組織文化として浸透しているか ・ 心理的安全性とコミュニケーションが、インシデント報告や改善提案を促す風土になっているか ・ “責任追及型”ではなく“学習・改善型”の文化が根づいているか	・ ポリシー（GV.PO）
7.共通の価値観 （Shared Value）	セキュリティ文化・理念・行動規範 ・ 自社がサイバーセキュリティに取り組む意義は何か（ビジョン、ミッション） ・ 組織のミッション・バリューに、セキュリティに関する価値観が明確に位置付けているか ・ 組織内でその価値観が共有され、日常の行動規範に落とし込まれているか ・ ステークホルダー（顧客、取引先、社会）への責任としてセキュリティを捉えているか ・ 価値観が施策や投資判断に反映される仕組み（方針、会議体、評価）があるか	・ ポリシー（GV.PO）

※JCIC 作成

付録２：サイバーセキュリティ・リスクマネジメント領域におけるリスクマネージャの主な役割

１．戦略を策定する

- 国内外の法令・制度等の動向とその影響、技術・標準・事例等の情報収集・分析・適用検討・報告
- 現状とあるべき姿のギャップ分析、戦略立案・策定、戦略効果測定・改善、経営への報告

２．制度を設計・維持する

- グループ規定、個社規定の制定、各種ルール等の維持・管理（制定・改廃・周知）
- グループ内リスク管理体制の設計・維持

３．戦略や施策を推進する

- 推進体制の設計・維持、関連部門間の調整、PDCA 設計・運用
- リスクマネジメントレベルを維持するための仕組みの設計・運用
- ステークホルダーからの信頼獲得のための情報発信
- 個別推進施策の企画・実行・効果測定・改善

４．教育・訓練・演習を企画・実施する

- 全社員向け研修・演習・訓練の企画・制作・実施・フォローアップ
- 対象別個別研修・演習・訓練の企画・制作・実施・フォローアップ

５．モニタリングする

- モニタリングおよびレビュー

６．インシデントに対応・監督する

- 事故対応（受付・初動・対応指導・監督官庁報告・再発防止策の確認と指導・横展開）
- インシデント対応組織の運用（リスク対策会議／リスク対策本部／災害対策本部／CSIRT 等）
- リスクコミュニケーション、レピュテーションリスクマネジメント

７．監査・外部評価を活用する

- 第三者評価制度、評価基準を用いた客観的なアセスメント等の活用

※筆者作成

サイバーリスクマネージャについては、今後あらためて別稿にて深掘りしていく予定である。

[本調査に関する照会先]

客員研究員 澤田雅広 sawada@j-cic.com

JCIC 事務局 info@j-cic.com