サイバー攻撃は"経営リスク":なぜ今、取締役会レベルでの対策が必須なのか

はじめに:サイバーセキュリティは「IT部門の問題」ではなくなった

「サイバーセキュリティは情報システム部門に任せておけばよい」——そう考える経営者は、もはやこの時代にはいません。2024年から2025年にかけて、日本企業を襲った大規模なサイバー攻撃は、企業経営の根幹を揺るがす事態へと発展し、サイバーセキュリティが単なる技術的課題ではなく、まぎれもない「経営リスク」であることを明確に示しました。

アサヒグループホールディングスやアスクルといった日本を代表する大企業が相次いでランサムウェア攻撃の被害に遭い、基幹業務の停止や物流の混乱を引き起こしました。ある大手企業では、サイバー攻撃により売上で83億円、営業利益で47億円というマイナスを計上。アサヒグループホールディングスに至っては、最大90億円もの損失が見込まれる事態となっています。

これらの事例は、サイバー攻撃が企業の事業継続性、財務状況、そして社会的信頼に直結する重大な経営リスクであることを如実に物語っています。そして今、このリスクに対する責任が、取締役会という企業統治の最高意思決定機関にまで及んでいるのです。

サイバーリスクの現状:増大する脅威と深刻化する被害

被害額の実態

日本におけるサイバー攻撃の被害は、年々深刻化の一途をたどっています。トレンドマイクロの調査によれば、国内企業がランサムウェア攻撃によって被った平均被害額は約2.2億円にものぼります。また、日本ネットワークセキュリティ協会(JNSA)の調査では、ランサムウェアの平均被害金額は約2,386万円、内部工数は平均27.7人月とされています。

さらに衝撃的なのは、過去5年間で損失を公表した52社の累計損失額が約118億円に達し、1社当たりの平均被害額が2億2,000万円を超えているという事実です。中小企業においても数千万円規模の被害が報告されており、もはや企業規模を問わずすべての組織がサイバー攻撃のターゲットとなっています。

攻撃の巧妙化と多様化

現代のサイバー攻撃は、かつての無差別的な攻撃から、特定の企業や組織を狙った高度な標的型攻撃へと進化しています。特にランサムウェア攻撃においては、単にデータを暗号化して身代金を要求するだけでなく、機密情報を窃取して公開すると脅迫する「二重脅迫」の手法が主流となっています。

2024年の統計では、1日あたり約330万回ものサイバー攻撃が検知されており、その数は前年比154%増加しています。サプライチェーンを通じた攻撃、内部関係者による情報漏洩、クラウドサービスの脆弱性を突いた攻撃など、攻撃手法は多様化の一途をたどっています。

被害の多面性

サイバー攻撃による被害は、単に金銭的損失にとどまりません。基幹システムの停止による業務の中断、顧客情報の漏洩による信頼の失墜、株価の下落、取引先との関係悪化、さらには訴訟リスクなど、その影響は企業活動のあらゆる側面に及びます。

ある出版大手企業では、ランサムウェア攻撃により数週間にわたって業務が停止し、書籍の配送や新刊の発売が遅延する事態となりました。このような事業継続性への影響は、短期的な売上減少だけでなく、長期的なブランド価値の毀損にもつながります。

取締役の法的責任：善管注意義務とサイバーセキュリティ

善管注意義務の範囲

会社法第330条および民法第644条に基づき、取締役は会社に対して「善良な管理者の注意義務」（善管注意義務）を負っています。この善管注意義務は、経営者として通常払うべき注意を怠らずに、会社のために誠実に職務を行う義務を意味します。

そして現代において、サイバーセキュリティ体制の構築と運用は、この善管注意義務の重要な一部として明確に位置づけられています。取締役がサイバーセキュリティに関する体制整備を怠ったことが原因で企業に損害が発生した場合、善管注意義務違反として損害賠償責任を問われる可能性があるのです。

内部統制システムの構築義務

会社法第348条第3項第4号および第362条第4項第6号は、取締役（会）に対して内部統制システムの構築を義務づけています。サイバーセキュリティ対策は、この内部統制システムの中核をなす要素の一つです。

大阪地方裁判所の判例では、取締役は会社の業務の適正な確保をするために必要な体制（内部統制システム)の整備をする義務を負うとされています。サイバーセキュリティ体制が企業規模や業務内容に照らして適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して善管注意義務違反による賠償義務を負うことになります。

監督責任と個人責任

WTW（ウイリス・タワーズワトソン）の調査によれば、サイバー攻撃後、組織の取締役や経営幹部が罰金、懲役、失職などの責任を負うケースが増加しており、回答者の51%がそのような事例を認識しています。

また、金融庁が2024年10月に改訂した「金融分野におけるサイバーセキュリティに関するガイドライン」では、経営陣がサイバーセキュリティを経営方針における重要課題の一つとして位置づけ、自らリーダーシップを発揮することが明記されています。経営陣がこの責任を怠った場合、善管注意義務違反や任務懈怠による損害賠償責任を問われ得るとしています。

サイバーセキュリティ経営ガイドラインが示す経営者の役割

ガイドラインの意義

経済産業省と独立行政法人情報処理推進機構（IPA）は、2023年3月に「サイバーセキュリティ経営ガイドライン Ver 3.0」を公表しました。このガイドラインは、大企業および中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある事項を体系的に示しています。

6年ぶりの改訂となった本ガイドラインでは、巧妙化した昨今のサイバー攻撃に備えるには、事前対策のみならず事後対策が必要であると明確に言及しています。これは、完璧な防御は不可能であることを前提に、被害を最小限に抑え、迅速に復旧できる体制を整備することの重要性を示しています。

経営者が認識すべき**3**原則

ガイドラインでは、経営者が認識すべき以下の3つの原則を掲げています。

原則**1**：経営者はサイバーセキュリティリスクを認識し、リーダーシップによって対策を進める

サイバーセキュリティは経営課題であり、IT部門だけの問題ではありません。経営者自らがその重要性を理解し、組織全体に対策の必要性を明確に示すことが求められます。

原則**2**：自社および系列企業、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施

現代の企業活動は、多くのビジネスパートナーとの連携によって成り立っています。自社だけが対策を講じても、サプライチェーン上の他社が攻撃を受ければ、自社の事業にも影響が及びます。エコシステム全体でのセキュリティレベルの向上が不可欠です。

原則**3**：平時および緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報の開示など、関係者との適切なコミュニケーションの実施

ステークホルダーとの信頼関係を維持するためには、適切な情報開示とコミュニケーションが欠かせません。インシデント発生時の迅速かつ透明性のある対応は、企業の信頼性を左右する重要な要素となります。

重要**10**項目の実践

ガイドラインでは、経営者が情報セキュリティ対策を実施する上での責任者となるCISO（Chief Information Security Officer：最高情報セキュリティ責任者）等に指示すべき「重要10項目」を定めています。

1. サイバーセキュリティリスクの認識、組織全体での対応の策定
2. サイバーセキュリティリスク管理体制の構築
3. サイバーセキュリティ対策のための資源（予算、人材等）確保
4. サイバーセキュリティリスクの把握と実現するセキュリティレベルの検討
5. サイバーセキュリティリスクに対応するための仕組みの構築
6. サイバーセキュリティ対策における PDCAサイクルの実施

7. インシデント発生時の緊急対応体制の整備
8. インシデントによる被害に備えた復旧体制の整備
9. ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策および状況把握
10. サイバーセキュリティに関する情報の収集、共有および開示の促進

これらの項目は、予防から検知、対応、復旧に至るまでの包括的なセキュリティマネジメントを求めるものであり、取締役会レベルでの監督と意思決定が不可欠となります。

取締役会が果たすべき役割

リスクの可視化と評価

取締役会は、まず自社が直面するサイバーセキュリティリスクを正確に把握し、評価する必要があります。これには、保有する情報資産の棚卸し、想定される脅威の分析、現状の対策レベルの評価などが含まれます。

Protivitiの「2024年のトップリスク」調査では、ランサムウェアを含むサイバー攻撃の脅威を管理するための備えが十分ではない可能性が指摘されています。多くの組織が、中核事業の中断やブランドの毀損などをもたらす可能性のあるサイバー攻撃への対応準備が不足しているのです。

取締役会は、定期的にサイバーセキュリティリスクの状況報告を受け、経営戦略や事業計画との整合性を確認しながら、必要な対策の方向性を決定する役割を担います。

適切な経営資源の配分

サイバーセキュリティ対策には、適切な予算配分と人材の確保が不可欠です。しかし、多くの企業では、セキュリティ対策が「コスト」として認識され、十分な投資がなされていないのが現状です。

取締役会は、サイバーセキュリティ対策を「投資」として位置づけ、事業継続性を確保し、企業価値を守るための重要な経営判断として、必要な予算を承認する責任があります。また、専門性を持った人材の採用・育成についても、取締役会レベルでの支援が求められます。

PwCの調査では、金融機関を含む重要インフラを対象としたサイバー攻撃が相次いでおり、企業業績に影響する被害が今後も懸念されるとしています。こうしたリスクを踏まえれば、セキュリティへの投資は企業の持続可能性を担保する必須の経営判断と言えるでしょう。

ガバナンス体制の整備

取締役会は、サイバーセキュリティに関するガバナンス体制を整備し、その実効性を監督する責任を負います。具体的には、以下のような取り組みが必要です。

CISOの任命と権限の付与：サイバーセキュリティの最高責任者として、CISOを任命し、組織横断的な権限と責任を明確にします。CISOは、経営陣との定期的なコミュニケーションを通じて、セキュリティリスクの状況を報告し、必要な対策について助言する役割を担います。

リスク管理委員会の設置：取締役会の下に、サイバーセキュリティリスクを専門的に審議する委員会を設置することも有効です。これにより、より詳細な議論と迅速な意思決定が可能となります。

監査・監督機能の強化：監査役や社外取締役は、サイバーセキュリティリスク管理体制が適切に構築・運用されているかを独立した立場から監査・監督する役割を果たします。定期的な監査を通じて、形式的な対策に終わることなく、実効性のある体制が維持されているかを確認することが重要です。

インシデント対応体制の構築

サイバー攻撃は「起こるかもしれない」リスクではなく、「必ず起こる」前提で備えるべきリスクです。取締役会は、インシデント発生時の対応体制を事前に整備し、その実効性を定期的に検証する必要があります。

インシデント対応計画（IRP：Incident Response Plan）の策定、CSIRT（Computer Security Incident Response Team）の設置、定期的な訓練の実施など、平時からの準備が求められます。また、インシデント発生時における意思決定権限、情報伝達ルート、ステークホルダーへの開示方針などを明確にしておくことが重要です。

サプライチェーンリスクへの対応

サプライチェーン攻撃の深刻化

近年、サプライチェーンを通じたサイバー攻撃が増加しています。これは、セキュリティ対策が比較的脆弱な中小企業やサプライヤーを攻撃の入口として、最終的に大企業や重要インフラに侵入する手法です。

経済産業省は、サプライチェーンを通じたセキュリティリスクの深刻化を受けて、企業のセキュリティ対策状況を可視化する新たな制度の検討を進めており、2026年10月以降の運用開始が予定されています。この制度は、取引先を含めたセキュリティレベルの「見える化」を推進し、企業間での信頼性の担保を目指すものです。

取引先管理の重要性

取締役会は、自社だけでなく、取引先やビジネスパートナーのセキュリティ対策状況についても把握し、必要に応じて改善を促す責任があります。具体的には、以下のような取り組みが考えられます。

セキュリティ基準の設定：取引先に求めるセキュリティ基準を明確にし、契約条項に盛り込みます。

定期的な監査：重要な取引先に対しては、定期的なセキュリティ監査を実施し、基準の遵守状況を確認します。

情報共有と支援：特に中小企業の取引先に対しては、脅威情報の共有や技術的支援を通じて、サプライチェーン全体のセキュリティレベル向上を図ります。

情報開示とステークホルダーとのコミュニケーション

透明性の確保

近年、企業のサイバーセキュリティに対する取り組みは、投資家、顧客、取引先など、さまざまなステークホルダーにとって重要な関心事となっています。特に上場企業においては、有価証券報告書や統合報告書において、サイバーセキュリティリスクとその対応状況を開示することが求められるようになっています。

取締役会は、自社のサイバーセキュリティに関するポリシー、対策状況、過去のインシデントとその対応、今後の計画などについて、適切な範囲で情報を開示し、ステークホルダーとの信頼関係を構築する必要があります。

インシデント発生時の対応

万が一、サイバーインシデントが発生した場合、迅速かつ適切な情報開示が企業の信頼性を左右します。隠蔽や遅延は、二次的な風評被害や株価の下落、さらには法的責任の追及につながりかねません。

取締役会は、インシデント発生時の情報開示方針を事前に定め、いつ、誰が、どのような内容を、どの媒体を通じて公表するかを明確にしておく必要があります。また、関係当局への報告義務についても、法令に基づいて適切に対応することが求められます。

今後の展望：規制強化と社会的責任

規制環境の変化

サイバーセキュリティに関する規制は、国内外で強化の方向にあります。2025年4月からは、ECサイト運営者に対してセキュリティガイドラインに基づく対策の実施が義務化され、特に脆弱性診断の実施が求められるようになります。

また、個人情報保護法の改正や、EUの一般データ保護規則（GDPR）など、データ保護に関する国際的な規制も厳格化しています。これらの規制に違反した場合、巨額の罰金や刑事責任を問われる可能性があります。

取締役会は、こうした規制環境の変化を常に把握し、コンプライアンスを確保するための体制を整備する責任があります。

ESGとサイバーセキュリティ

近年、ESG（環境・社会・ガバナンス）投資の観点から、企業のサイバーセキュリティへの取り組みが評価されるようになっています。特に「ガバナンス」の要素として、適切なリスク管理体制の構築は重要な評価項目となっています。

投資家は、サイバーセキュリティリスクが適切に管理されていない企業に対して、投資を控えたり、株主提案を通じて対策の強化を求めたりするケースが増えています。取締役会は、ESG の

観点からも、サイバーセキュリティ対策を企業価値向上の重要な要素として位置づける必要があります。

社会的責任としてのセキュリティ

企業は、自社の利益を追求するだけでなく、社会の一員として公共の利益に貢献する責任を負っています。サイバーセキュリティ対策もまた、顧客や取引先の情報を守り、社会インフラの安定性を維持するという社会的責任の一環です。

特に重要インフラを担う企業や、大量の個人情報を扱う企業においては、自社のセキュリティ対策の不備が社会全体に甚大な影響を及ぼす可能性があります。取締役会は、こうした社会的責任を深く認識し、高いレベルのセキュリティ対策を実施することが求められます。

実践への第一歩：取締役会が今すぐ取り組むべきこと

現状把握とギャップ分析

まず、自社のサイバーセキュリティ対策の現状を正確に把握することから始めましょう。「サイバーセキュリティ経営ガイドライン Ver 3.0」の重要10項目をチェックリストとして活用し、現状とあるべき姿とのギャップを明確にします。

IPAが提供する「サイバーセキュリティ経営ガイドライン Ver 3.0実践のための手引き」など、支援ツールを活用することで、段階的に対策レベルを向上させることが可能です。

取締役会での定期的な議論

サイバーセキュリティを取締役会の定例議題とし、定期的に状況報告を受け、議論する体制を整えます。CISOや情報セキュリティ部門の責任者から直接報告を受けることで、経営層と現場との認識のズレを防ぐことができます。

外部専門家の活用

サイバーセキュリティは高度に専門的な領域であり、社内だけで対応することには限界があります。外部の専門家やコンサルティング会社の知見を活用し、客観的な評価と助言を得ることが重要です。

また、サイバー保険の加入も、リスクの移転手段として有効です。ただし、保険はあくまで事後的な金銭的補償であり、根本的な対策を怠る理由にはなりません。

教育と意識向上

サイバーセキュリティ対策は、技術的な対策だけでは不十分です。従業員一人ひとりがセキュリティ意識を持ち、適切な行動を取ることが不可欠です。

取締役会は、経営層自らが率先してセキュリティ教育を受け、組織全体に対してその重要性を示すことで、企業文化としてのセキュリティ意識を醸成する必要があります。

結論：サイバーセキュリティは経営の最重要課題

デジタル化が加速する現代において、サイバーセキュリティは企業の持続可能性を左右する最重要課題となっています。サイバー攻撃による被害は、金銭的損失にとどまらず、事業継続性、社会的信頼、そして企業価値そのものを脅かします。

取締役には、会社法に基づく善管注意義務として、適切なサイバーセキュリティ体制を構築し、運用する法的責任があります。この責任は、もはや情報システム部門やセキュリティ担当者だけが負うものではなく、取締役会という経営の最高意思決定機関が主体的に取り組むべき課題なのです。

「サイバーセキュリティ経営ガイドライン Ver 3.0」が示す3原則と重要10項目は、取締役会がこの責任を果たすための具体的な指針を提供しています。経営者自らがリーダーシップを発揮し、サプライチェーン全体を視野に入れた対策を講じ、ステークホルダーとの適切なコミュニケーションを図ることが求められています。

サイバーリスクは日々進化し、新たな脅威が次々と出現しています。完璧な防御は不可能であるという前提のもと、継続的な改善と、インシデント発生時の迅速な対応体制を整備することが重要です。

取締役会レベルでのサイバーセキュリティ対策は、もはや選択肢ではなく、企業が社会において事業を継続するための必須要件です。今この瞬間も、あなたの会社は、見えない脅威に晒されています。明日、あなたの会社がサイバー攻撃の標的となったとき、取締役会として適切な対応ができる体制は整っていますか？

その問いに対する答えが、これからの企業の未来を決定づけるのです。

監修者

鎌田光一郎

青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先

Librus株式会社（代表取締役 鎌田光一郎）

〒105-0004 東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F

TEL: 03-6772-8015

お問い合わせフォーム：https://librus.co.jp/contact