特集 **経営リスクとしてのサイバー脅威**

「危機」「変化」「統治」サイバーリスクを経営課題として捉える３つの観点



池田泰徳

経営者への問い

2025年、国内大手製造業や食品関連企業でランサムウエア（身代金要求型ウイルス）攻撃による基幹業務の長期停止が相次いだ。いずれも侵入口となったのは、自社システムへの接続点であるVPN機器、グループの地方・海外拠点、サプライチェーンを構成する委託先などの「セキュリティの隙」からであった。受注・出荷の停止による影響は、財務的損失にとどまらず、顧客への供給責任の毀損や社会的信用の低下として経営全体へ波及した。

ほかにも、医療機関や重要インフラ事業者で、サイバー攻撃を端緒とするシステム障害が社会サービスへの影響として表面化した事例など、枚挙にいとまがない。これらの事象は、攻撃による被害の波及範囲が単一企業の業務システムにとどまらず、業界全体・社会インフラにまで及び得る危機的な構造になっていることを露呈させている。

さらに、攻撃の高度化はもとより、ビジネス化・民主化が進んでおり、国家支援型攻撃なども出現し、動機も金銭目的にとどまらず、経済的競争や国際政治的な思惑と連動する事例が増えている。そのため、近年のサイバー攻撃は、特定業種や大企業だけの問題ではなく、業種・規模を問わず多くの経営者が「自社も同じ立場になり得る」と向き合うべき現実的な課題となっている。本稿はこの経営課題を「危機」「変化」「統治」の３つの観点から整理し、経営者が今何を見据え、何を決断すべきかを論じる。

３つの観点で捉えるサイバーリスクの全体像

経営課題としてサイバーリスクに対処する際、多くの企業に共通することがある。目前で起きている「危機」への対処に追われるあまり、「変化」を見落とし、経営としての「統治」設計にまで至れないという課題である。この３つの観点の欠落こそが、甚大な被害へ至る最大の落とし穴であろう。

本特集では、「危機」「変化」「統治」の３つの観点を次のように定義した。

「危機」とは、今まさに経営を直撃する、現在進行形の喫緊の脅威である。ランサムウエアとサプライチェーンを経由した侵害がここ

に属する。被害の実態はもはや「一時的なシステム停止」にとどまらず、数カ月にわたる業務停止と多大な損失を招く経営直撃型の危機へと変質している。

「変化」とは、外部環境そのものが変わりつつある中長期のうねりである。深刻化する国家間サイバー競争と重要インフラへの組織的攻撃に対応するため、いわゆる経済安全保障推進法、重要経済安保情報保護活用法、サイバー対処能力強化法という三法が2022年から2025年にかけて整備された。さらに2026年にはフロンティアAI（最先端の大規模AI）の急速な能力向上が顕在化し、攻撃構造を質的に変えるという新たな次元の変化も加わっている。このような外部環境の構造変化が進行する中、これらの「変化」を迅速に捉え、先を見据えた対策を講じていく必要がある。

「統治」とは、２つの観点を踏まえて対処する、永続的な経営課題である。ガバナンスの設計と経営としての意思決定の構えがここに位置づけられる。「危機」と「変化」を俯瞰しながら継続的かつ機動的に判断を下す仕組みが、統治の実体である。

これらの３つの観点は不可分ではなく、積み重なる構造でありながら、相互に影響し合っている。たとえば、ランサムウエア攻撃による委託先を経由した侵入という喫緊の課題は、一義的には「危機」と捉えられるが、この状況を受けたサプライチェーン対策評価制度（SCS評価制度）の創設は「変化」と捉えることができ、それらを踏まえたサプライチェーン管理やセキュリティ対策の中長期的な方針策定などは「統治」と捉えることができる。また、「変化」としてその兆候が表れた事象が喫緊の課題となり、「危機」として対応する必要が出てくる可能性も高い。これらの観点は深く関連しており、そこに「統治」設計が欠けていれば、組織は適切なセキュリティ統治を行うことができない。

本特集は４本の論考で構成するが、以下ではこれらを「危機」「変化」「統治」の観点から総括し、その位置づけを整理したい。

企業価値を守るランサムウエア対策

第一論考は、攻撃がいかに経営直撃型の脅威へと変質したかを、国内の実被害事例から詳述する。主に、「危機」とその「統治」を軸とした論考である。

攻撃の拡大を加速させているのが、Ransomware as a Service（RaaS：攻撃ツールやインフラを開発者が提供し、実行者が分業で攻撃する形態）の普及である。高度な技術を持たない攻撃者でも大規模な被害を与えることが可能となり、攻撃件数は高水準で推移している。

また、被害事例が示すのは復旧の長期化という現実である。バックアップ自体が暗号化・削除される事例が相次ぎ、主要サービスの復旧に数カ月を要したケースも出ている。被害企業の多くは対策製品を導入していたが、攻撃者はそれによる検知をすり抜けた。

第一論考ではこうした実態を踏まえ、「侵入前提」の発想への転換を説く。侵入を前提とした技術的な備え、迅速な初動対応を可能とする組織体制、そして意思決定を担う経営の関与が連動して初めて実効性を持つ。

取引先のセキュリティは「自社のリスク」である

第二論考は、サプライチェーン攻撃が発注

者・受注者の双方に被害をもたらす構造を体系的に整理する。前述のとおり、ランサムウエア対策とは深く関連することから、喫緊の課題としての「危機」を基盤としつつ、制度動向への対応としての「変化」「統治」を軸とした論考となる。

攻撃者から見ると、堅固に守られた大企業を正面突破するより、防御の薄い委託先を踏み台とし、側面／裏口から侵入する方が効率的である。委託先１社への侵害が委託元の顧客情報の流出に直結し、金融機関や自治体など多数の組織に被害が連鎖した事例は、この論理の例証を示している。自社のセキュリティが万全でも、対策が手薄な委託先が起点となってコア事業が全面停止する。それが今日の実態である。

こうした課題に対応するため、経済産業省および内閣官房国家サイバー統括室は、サプライチェーン強化に向けたSCS評価制度の構築方針を2026年３月に公表した。発注者・受注者双方の負担を軽減しながら、サプライチェーン全体のセキュリティ水準を客観的に可視化することを目的とする制度である。第二論考は制度の詳細に加え、今すぐ着手できる３つの基礎的な対策、すなわち、委託先のセキュリティ対策状況の把握、アカウント管理台帳の棚卸し、バックアップの確認、を提示する。

フロンティアAI時代のサイバー安全保障

第三論考は、フロンティアAIの台頭やサイバー安全保障に関連する法整備の状況を踏まえ、経営者が着手すべき行動指針を提示する。「変化」および「統治」を軸とした論考である。

日本のサイバー安全保障法制の整備は、フロンティアAIの登場とは独立した経緯で進展した。2022年に成立した経済安全保障推進法を皮切りに、重要経済安保情報保護活用法、サイバー対処能力強化法という三法が相次いで成立し、重要インフラの調達審査・機微情報の保全・官民情報共有の枠組みが形成された。これらは深刻化していた国家間サイバー競争と重要インフラへの組織的攻撃に対応するものとして立案された。

しかし三法の整備が進む最中の2026年４月、既存の前提を揺るがす新たな事態が生じた。あるAI開発企業の最先端モデルが数週間で数千件のゼロデイ脆弱性（未公開の未修正脆弱性）を自律的に発見したとされ、攻撃能力の飛躍、脆弱性の公開から悪用までの時間軸の圧縮など、大きな環境変化が起きた。これを受け、政府は三法の枠組みを土台として2026年５月に14省庁連名の「Project YATA-Shield」を機動的に発出し、フロンティアAIの悪用リスクを前提に、同技術を防御に積極活用するという二面戦略を明示した。

2030年のサイバーセキュリティ

第四論考は、個別脅威への点的対応ではなく、2030年に向けた構造変化の景観（ランドスケープ）を俯瞰し、経営判断の見取り図を提示する。これは、さまざまな「変化」の見極めと、「統治」へのつなげ方の処方箋を提示した論考である。

第１の変化は、セキュリティインシデントが経営において「災害」と同等の備えを要する事象になるという点である。米国での事故事例などから、一組織への攻撃が社会インフ

ラを止める現実を示す。そこからIT部門が管掌する「IT-BCP（ITシステムの事業継続計画）」のスコープを超え、経営トップが意思決定主体となる「サイバーレジリエントBCP」への転換を提言する。

第２の変化は、エマージングテクノロジー（新興技術）の社会実装に伴う「ちょうどいい」リスクガバナンスが求められるという点である。AI・量子・ロボティクスなどの新興技術がもたらす不確実性は、ネガティブなリスクであると同時に先行実装企業が競争優位を得るポジティブなリスクでもある。変化する状況に組織が自律的に最適対応できるガバナンスへの進化が求められる。

第３の変化は、サイバーセキュリティが「社会技術的な事象」として捉えられるようになるという点である。技術だけでは対策できないいくつかの例を挙げながら、技術的対策と組織設計・ガバナンスを一体で設計する社会技術的アプローチの必要性を論じる。

第三論考の法制整備で述べた「変化」とここでいう技術的「変化」は独立した潮流ではない。法制はAIや量子の技術動向を見越して設計され、技術の変化が法整備を促し、法整備がまた技術対応の方向を規律する。このようにさまざまな「変化」は、複数の変化が重なり合う複合的な外部環境の構造変化として捉えるべきである。この全体を見渡し、経営判断の統治設計に落とし込むことが「統治」の本質である。

義務として問われる経営の統治

本稿で取り上げた「危機」も「変化」も、経営者の視野に入っていたはずが、それでも動けない組織が後を絶たない。その原因は、それぞれの対応を有機的・全社横断的に捉えず、個別の部署／組織が分断して捉えてきたことにある。ランサムウエアを「IT部門の事案」として処理し、法制対応を「コンプライアンス部門の案件」として切り出し、それぞれへの対応を個別に委ねてきたのではないか。

しかし、財務リスクを経理部門に丸投げする経営者はいない。サイバーリスクをセキュリティ担当者に委ねてきた慣行は、今や国際的な規制水準において通用しなくなっている。欧州のNIS2指令は経営層によるサイバーリスク管理の直接承認・監督を義務づけ、違反時には取締役の個人責任を問う。米国では重大インシデントの短期開示義務を通じ、経営の意思決定プロセスそのものが問われる構造が定着した。第三論考が指摘するとおり、経営者がサイバーリスクの管理状況を取締役会で説明できない状態は、日本においても善管注意義務違反に問われかねない状況にある。もはや先送りしている猶予はない。

セキュリティへの投資は「守り」のコストではなく信頼の証明であり、法制対応力は調達適格性の条件となり、SCS対応は取引先からの信頼を担保し、CISO体制の確立は投資家・市場への経営品質の証明となる。「危機」「変化」「統治」すべてを経営の俎上に乗せること、それがサイバーリスクを真に経営課題として制するための、最初の一歩である。

著者

池田泰徳（いけだやすのり）
NRIセキュアテクノロジーズ 代表取締役社長
専門はサイバーセキュリティに関するコンサルテーション、ソリューション全般、アイデンティティ、暗号など