World Trend Foresight

サイバーリスクの二重性モデル

2025 年 7 月

企業戦略と官民連携に活かす実践的枠組み

サイバー空間が組織活動の基盤となった現代において、悪意あるサイバー活動によって引き起こされる被害が多様化している。一言にサイバーリスクといっても、セキュリティソフトで自動的に処理される大量のスパムメールもあれば、国家安全保障に関わる重大インシデントまで、その性質も影響範囲も異なる「サイバーリスク」が併存する時代となった。こうした中、効果的なリスクマネジメントを実現するためには、単なる脅威一覧ではなく、意思決定に資する枠組みが求められる。その鍵となるのが、本稿で取り上げる『サイバーリスクの二重性（duality of cyber risk）』、すなわちサイバーリスクを特性に応じて「消耗的リスク（attritional risk）」と「壊滅的リスク（catastrophic risk）」に分解する枠組みである。

そこで本稿では、日本ではあまり馴染みのない「サイバーリスク二重性」の概念を解説し、「消耗的リスク」と「壊滅的リスク」という二軸でサイバーリスクを再整理する。さらにこの枠組みが、官民連携・企業戦略・非技術領域の議論活性化といった面でいかに有効であるかを論じたい。そのうえで、リスク分類を活用するうえでの留意点と今後の課題を提示し、最後に日本のサイバーセキュリティの発展に向けた提言を記す。

1. サイバーリスクの二重性（duality of cyber risk）とは何か

「サイバーリスクの二重性（duality of cyber risk）」という概念がある[1]。一般に「リスクの二重性」とは、頻度は高いが損害規模が小さいリスク（消耗的リスク: attritional risk）と、発生頻度は極めて低いが損失規模が極めて大きいリスク（壊滅的リスク: catastrophic risk）の 2 種類が同時に存在することを指す。この用語はもともと保険業界においてリスクを分類する際に用いられてきた概念であり、とりわけテロリズムや自然災害、健康リスクといった明確な物理的被害を伴う事象を取り扱うものであったが、サイバーリスクにも二重性を適用する必要性が議論されるようになってきている。その理由を、（1）サイバーリスクのヘビーテール[2]的特性、（2）経営判断および外部連携の必要性増に分解して述べる。

（1）サイバーリスクのヘビーテール的特性

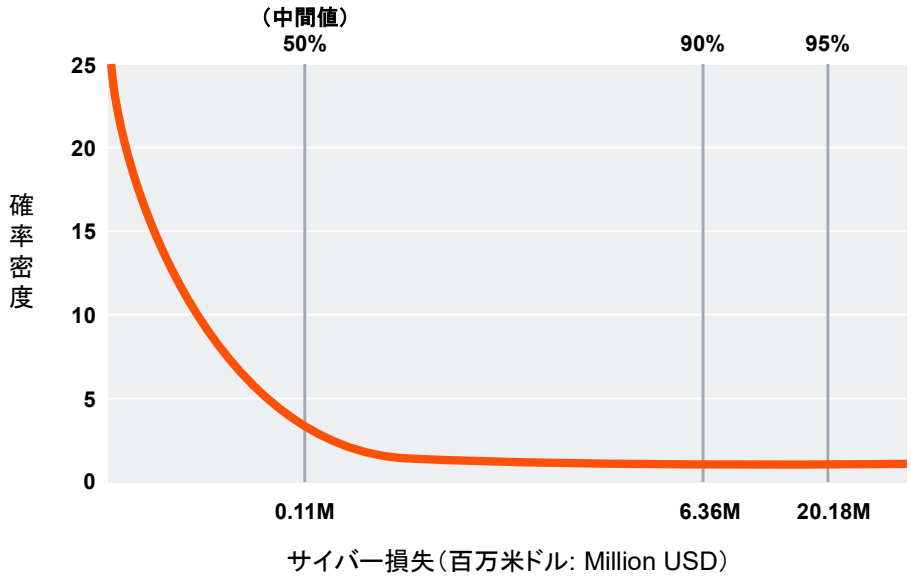
近年の研究と実務の進展により、サイバー空間のリスクにも二重性が存在することが分かってきている。サイバー関連の損失分析によれば、約 85%のインシデント損失は 2 百万米ドル未満に留まる一方で、ごく一部の事象が 10

[1] Romanosky, Sasha, Lloyd Dixon, R. J. Briggs, and Henry H. Willis (2025) *Insuring Catastrophic Cyber Risk*. Santa Monica, CA: RAND Corporation

[2] ヘビーテールとは、確率分布において非常に極端なイベントに対しても一定の確率が割り当てられる性質を指す。

億米ドルを超える巨額損失を引き起こしていることが示されている[3]。すなわち、サイバー損失分布はヘビーテール的特性を有し、極めてまれだが多大な損失を伴う事象が存在する（図表 1）。こうした分布特性は「一発の損失が組織を壊滅させ得る（One loss causes ruin）」ことを意味している。このことは、国家および組織運営において、サイバーリスクの「平均値」が必ずしも有効な指標とならず、極端値に対する備えが不可欠であることを意味している。この「二種類の極端なリスクが入り混じっている」という洞察は、日々大量に発生するセキュリティアラートや小規模なインシデントに対応しながら、いつ起こるかわからない大規模なセキュリティインシデントの発生に神経を尖らせているサイバーセキュリティ実務者の体感とも一致するであろう。

図表 1　サイバーイベントの損失額に対する分布の確率密度関数モデル



（出所）Shevchenko et al.(2022) のデータをもとに筆者作成。2008-2020 年に報告された主に米国でのサイバーイベントに基づく。

（2）経営判断および外部連携の必要性増

ビジネスや社会運営がサイバー空間への依存度を増すに伴って、サイバーリスクは IT 部門やセキュリティ技術者だけの問題ではなくなってきていることは論を俟たない。経営層はサイバー活動による財務損失、風評被害、法規制違反、事業中断などのリスクを幅広く検討する必要があり、意思決定の際にはサイバー活動による影響（outcome）に関する洞察が必要となる。そのような場面においては、数あるサイバーリスク分類方法の中でも「サイバーリスクの二重性」のように損害ベースの分類が投資判断に活用しやすい。また、内部リソースだけでは対応しきれない大規模なリスクシナリオを想定せざるを得ない以上、外部連携を前提としたサイバーリスクマネジメント手法も俎上に上がる。リスク移転を意図したサイバー保険はその典型であるが、上述の通り消耗的／壊滅的リスクの分類は保険業界を出自としているため、業界横断でサイバーリスクを議論する際の共通言語としても有用である。

[3] Pavel V Shevchenko, Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, and Stefan Trück. (2022) *The nature of losses from cyber-related events: risk categories and business sectors.* Journal of Cybersecurity

2.「消耗的リスク」と「壊滅的リスク」の違い

ここからは、サイバーリスクを「消耗的リスク」と「壊滅的リスク」に分類して、それぞれの違いを明確化する。以下はそれぞれの特徴の比較である（図表 2）。

図表 2　消耗的サイバーリスクと壊滅的サイバーリスクの比較

項目	消耗的リスク	壊滅的リスク
発生頻度	高頻度（日常的に発生）	低頻度（数年～十数年に一度）
損失規模	小規模（数千円～数億円未満）	大規模（数百億円以上）
影響範囲	単一組織または限定的なサプライチェーン	国家規模、業界横断、社会基盤全体
代表的な攻撃例	フィッシング、内部不正、ランサムウェアによる限定的な暗号化、情報漏洩、認証情報窃取	国家主体によるマルチドメイン作戦、APT 攻撃によるクラウド・インフラ停止、大規模なサプライチェーン被害、中央集権型システムへのゼロデイ攻撃
保険カバー状況	民間保険市場で対応可能（通常保険商品で引受）	保険市場では難しい場合が多く、再保険や政府支援が必要
対応策	サイバーハイジーンに則った標準的セキュリティ施策、SOC 運用、インシデント対応計画など	ガバナンスレベルの BCP、産業横断的な対応協定、官民連携のインテリジェンス共有
政策的介入の必要性	通常は不要（企業努力の範囲）	政府・規制当局の関与が必須
経営インパクト	単年度予算管理内で吸収可能	組織存続に関わる重大影響、業界全体の社会的信用喪失
例示的な事例	メール誤送信による情報漏洩、ビジネスメール詐欺による金銭的被害	ソフトウェア由来の世界規模のシステム停止、クラウドサービス侵害によるユーザーへの連鎖的被害、電力設備への高度なサイバー攻撃

（出所）筆者作成

（1）消耗的リスク

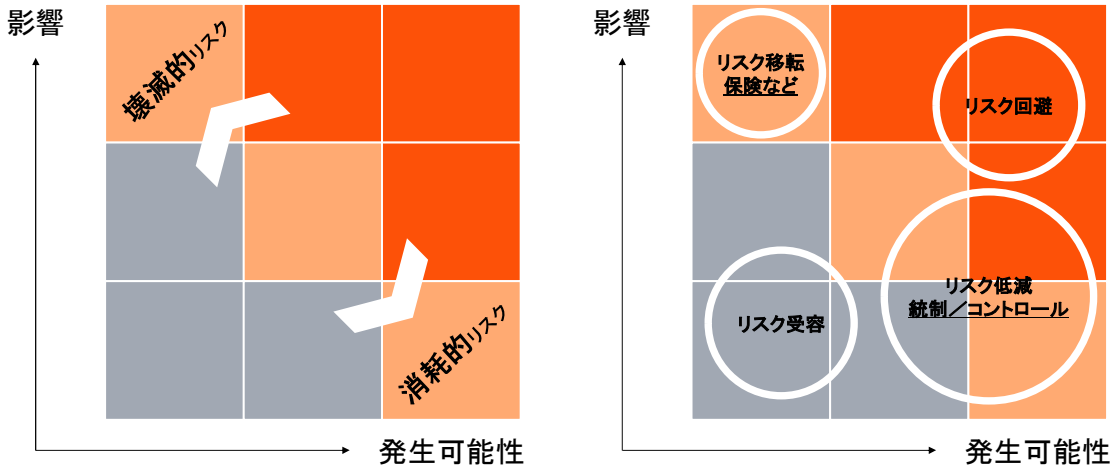
比較的高頻度で発生し、通常の事業運営や情報システムの安定性に日常的な影響を及ぼす小規模なサイバーリスク群を指す。典型例として、従業員のメール誤送信による小規模な情報漏洩、フィッシングメールによる認証情報の窃取、サービス拒否（DoS）攻撃によるサーバーの一時停止などが該当する。サイバー活動による被害規模は限定的で、個別企業が吸収できる範囲に収まる。リスク要素に関する過去データ（損失データやシグニチャ情報など）が存在するため、セキュリティコントロールによるリスク発生の低減が可能であり、通常はサイバー保険がある程度適用可能である。

(2) 壊滅的リスク

発生頻度は極めて低いものの、ひとたび発生すれば企業の存続や業界全体、あるいは社会基盤・国家安全保障にまで影響を及ぼす高インパクトなサイバーリスク群を指す。例えば、都市運営を支える重要インフラ(電力・交通・金融など)の制御システムに対する標的型攻撃、サプライチェーンの中核的 IT 製品・サービスに対するゼロデイ攻撃、多国籍クラウドサービスプロバイダーに対する超高負荷の DDoS 攻撃などが含まれる。こうしたリスクは、複数の組織・社会が連鎖的に損害を被る現象であり損害規模は数百億円以上に達する。それゆえ既存のサイバー保険のスキームでは対応しきれないケースが多い。

上記の分類を「リスクマトリクス[4]」に当てはめると新たな示唆が得られる(図表 3)。一般的に、リスクマトリクスにおいては「発生可能性高かつ影響大」を『高リスク(赤色マス部分)』、「発生可能性低かつ影響低」を『低リスク(灰色マス)』として評価し、それ以外を『中リスク(橙色マス)』として扱う。したがって、その評価基準に則ると、消耗的リスクは図の右下、壊滅的リスクは左上に位置づけられ、いずれも『中リスク』として評価される。つまり、リスクマトリクスの枠組みに基づけば、サイバーリスクは本質的に『中リスク』内に分布しており、その分布をどう捉えるかがサイバーセキュリティを成功に導く論点となる。さらに言えば、高リスクおよび低リスクに関しては、該当リスクを回避する、受容するという「決断」そのものがリスク対応策となるが、中リスクに対しては該当リスクを移転する、低減するといった「行為」がリスク対応策になるという相違点の理解も、建設的な議論には欠かせない。

図表 3 「消耗的リスク」と「壊滅的リスク」のリスクマトリクス上の位置付けとリスク対応策



(出所)筆者作成

一点、消耗的／壊滅的リスクの分類をサイバーリスクに適用するにあたっての注意点がある。それは、一見すると消耗的リスクに分類される事象でも、条件次第で壊滅的な様相を呈する場面があることだ。例えば昨今のランサムウェア攻撃は特定企業を狙う傾向にあるが、自己増殖するワーム的手法やサプライチェーンを通じた同時攻撃が行われれば、多数の企業が同時に身代金要求被害に遭う大規模感染が発生し得る。2017 年に世界中の多数組織に同時多発的に被害を与えた「NotPetya」や「WannaCry」は、ランサムウェアの破壊力とワームの増殖力が組

[4] リスクマトリクス(Risk Matrix)とはリスク評価手法の 1 つで、発生可能性と影響度を軸としてリスクを図式化したもの。

み合わさり、システミックなサイバー災害となった事例である[5, 6]。また、個別には小規模にとどまる脆弱性も、もしそれが広く普及した共通ソフトウェアの未知の脆弱性（ゼロデイ）であれば、偶発的・意図的を問わずそれが突如悪用された場合に世界規模で連鎖的な損害を生む可能性がある。このように、平時は独立した消耗的リスクであっても特定の条件下で壊滅的リスクに転嫁する潜在性を持つ事象が存在する。言い換えれば、消耗的リスクを軽減するための基本的なサイバーセキュリティ活動が、壊滅的リスクの発生と損害規模低減に寄与しているということでもある。サイバーハイジーン（基本的なサイバー衛生習慣）に代表される消耗的リスク低減のアプローチは決して派手ではないが、その重要性はいくら強調してもしすぎることはない。

3. 二重性に基づくサイバーリスクマネジメントの利点

本節では、ここまでの議論を踏まえて、消耗的リスクと壊滅的リスクの二重性をサイバーリスクマネジメント戦略にインストールすることの利点を取り上げたい。以下に、（1）官民連携の枠組み設計、（2）民間企業における活用、（3）非技術的要素の取り込みという 3 つの観点から整理する。

（1）官民連携の枠組み設計：役割の明確化

民間企業においてサイバーセキュリティを議論する場合、その大部分は消耗的リスクへの対応が焦点となる。消耗的リスクは過去データに基づく対応策や予見可能性もあるため、PDCA に基づく運用が可能である。また、サイバーセキュリティ活動を投資対効果によって評価・改善することができるため、営利目的の企業活動との相性が良い。そのため、主に防御主体である民間企業が主導するかたちでサイバーハイジーンの徹底や、SOC（Security Operation Center）の強化、従業員教育を行うことが推奨される。

一方で、壊滅的リスクへの備えには、政府・民間企業・学術機関の三者協働が不可欠となる。サイバーリスクはその性質上、国家レベルの安全保障や社会経済の安定性に波及し得るため、個別企業が防御を強化するだけでは対応しきれない局面が存在する。こうした壊滅的リスクに対しては、政府の介入や支援、産官学連携のタスクフォースの設置が求められる。壊滅的リスクの発生時には公共インフラや国家機能そのものを脅かす可能性があるため、必然的に国家安全保障の文脈でのサイバーセキュリティが求められることとなる。したがって、このリスクマネジメント活動の主導者は国家機関となり、公共政策の整備や国家規模でのレジリエンス強化に焦点を当てた活動が行われる。米 CISA（Cybersecurity and Infrastructure Security Agency: 米サイバーセキュリティ・インフラセキュリティ庁）が推進する「Systemic Cyber Risk Reduction Venture[7]」は政府主導の壊滅的リスクへの官民協働対策の好事例であり、国家重要機能（NCF）のリスクマッピングや、民間企業との共同リスク評価を通じて、全社会的なシステミックリスクの低減を目指している。

（2）民間企業における活用：セキュリティ戦略への応用

企業経営層や CISO にとっても、二重性の視点は戦略の成熟度を高める有力な枠組みとなる。それぞれのリスク特性に応じて、原則・目標・対応シナリオを明確に設定することで、リスクマネジメント体制の整合性が向上し、投資判断の最適化に寄与する。例えば、消耗的リスクは毎年のコスト・ベネフィット分析（セキュリティ投資や保険料）で管理することを前提として、分析フレームワークとして JCIC が提案する「連結売上高の 0.5%をセキュリティ投

[5] Proofpoint. “Petya (NotPetya)” https://www.proofpoint.com/uk/threat-reference/petya (2025 年 6 月 24 日にアクセス)

[6] National Cybersecurity and Communications Integration Center. “What is WANNACRY/WANNACRYPTOR?” https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf (2025 年 6 月 24 日にアクセス)

[7] CISA（2021）”Systemic Cyber Risk Reduction Venture”

資へ[8]」や、サイバーセキュリティ投資の代表的モデルである「ゴードン・ローブモデル[9]」を適用することが考えられる。また、サイバー保険の評価も両リスクの区分けが明確なほど容易になる。このように、二重性の視点を経営判断の共通言語とすることで、経営陣は「消耗的／破滅的サイバーリスク」の見極めのもとで予算配分や緊急投資判断を行いやすくなる。

また、壊滅的リスクへとサイバーレジリエンスの関係性も強調しておきたい。サイバーレジリエンスとは、つまるところサイバー活動に起因する壊滅的リスクへの組織の耐性・体制・態勢である。壊滅的サイバーリスクについては個社努力だけで被害を防ぎきることは難しいために、事前に最悪の事象を想定したシナリオ分析と演習を行うことが有益である。大規模停電や通信途絶、大規模なデータ消失といった極端なケースを想像し、経営層を含めた全社的訓練を積むことで、いざという時の混乱を最小限に抑え重要機能を維持する能力が養われる。広域で被害が発生する壊滅的リスクの特性上、同業他社や政府機関との協調体制を平時から構築しておくことも経営層に期待される。サイバーレジリエンスとは単なる技術的防御策の集合ではなく、リスクファイナンス・事業継続・経営判断を統合した包括的なリスクマネジメント態勢であり、その実現は消耗的・壊滅的リスクそれぞれの低減に向けたミクロ（自社内部）とマクロ（産業横断・産官学連携）の融合である。

(3) 非技術的要素の取り込み：統合領域への進化

サイバーセキュリティは元来コンピューターサイエンスの一分野として発展してきたため、技術的・運用的側面（マルウェア解析、ソフトウェア脆弱性分析、暗号技術など）に議論が集中しがちであった。しかし、現代のサイバー空間は国家運営、産業構造、国民生活のあらゆる側面と密接に結びついており、その結びつきは今後も強まることはあるにせよ弱まることはない。いまやサイバーセキュリティ領域全体の成長には、経済的および社会的利益を両立させる必要があるため、幅広い視点からの連携が求められてきている[10]。サイバーセキュリティは高度な技術的要素だけではなく、政策・法務・経営・社会科学といった多様な専門知識を統合的に扱うべき領域であると言える。

「サイバーリスクの二重性」への備えは、サイバーセキュリティの「非技術的要素」の重要性を強調する。リスク特性に応じた例を見てみよう。活動に対する投資対効果や運用持続性が重要視される消耗的サイバーリスクへの対処には、リスク投資判断や損益分析を専門とする経営・財務分野や、社員のセキュリティ意識向上や組織文化改革、ソーシャルエンジニアリングへの対策設定に優れた心理・社会科学分野が重要な役割を果たす。社員行動を制約する規範設定などの人間行動に焦点を当てたセキュリティ活動においてはとりわけ重要である。また、今後のAI 技術の浸透を考えると、消耗的リスクへの技術的対抗策は自動化される流れにあるため、人間が為すべきサイバーセキュリティ活動の大部分は、倫理的・政治的な判断が求められることになる可能性が高い。現在の多くの組織において、「情報の機密性をどのように担保するか」に加えて、「自社における機密性をどう定義するか」や「機密性の定義をどのように従業員に浸透させるか」が論点になってきていることはその一例であろう。壊滅的リスクへの対処に関しては、前述の通りマクロな視野と広範囲のコミュニケーションが不可欠となるため、「サイバーセキュリティ」という領域よりも上位にあたる「エンタープライズ・リスク・マネジメント（ERM）」や「事業継続計画（BCP）」といったレイヤーに踏み込むことになる。その意味では、サイバーセキュリティ実務者、特に CISO は連携先となる専門家に適したかたちでサイバーリスクを「翻訳」するインターフェースとしての役割を求められるだろう。

[8] Japan Cybersecurity Innovation Committee (2022) “社内のセキュリティリソースは「0.5%以上」を確保せよ”

[9] Gordon, L., Loeb, M. and Zhou, L. (2016) *Investing in Cybersecurity: Insights from the Gordon-Loeb Model*. Journal of Information Security

[10] OECD. (2019) “Digital security and resilience in critical infrastructure and essential services”

4. サイバーリスク分類の留意点と課題

ここまで述べてきたように、サイバーリスクを「消耗的リスク」と「壊滅的リスク」に分けて整理する枠組みは、実務的な判断や政策設計において有用な視座を提供するものである。しかしその一方で、サイバーリスク分類を運用する際にはいくつかの留意点が存在する。本節では、留意点として「分類体系の特性考慮」に焦点を当て解説するとともに、分類体系のあり方と密接に関わってくる「サイバーイベントの統計情報」を今後の重要課題として提示する。

(1) 留意点: サイバーリスク分類体系の特性考慮

ここまでサイバーリスクの二重性分類の利点を提示してきたが、当然ながらこれがすべてを解決する万能フレームワークというわけではない。フレームワークである以上は、利用者の目的や条件によってその効果が変わってくる。優れた分類体系は、分析者やリスクハンドラーが効果的な低減策や手順を計画・実施するうえで大きな助けとなるが、不適切な分類体系を採用するとサイバーリスクの正確な把握や分析とそれに基づく意思決定が困難になる。リスクの分類方法にもそれぞれ特徴があることを理解したうえで活用することが肝要である。現時点では、以下の通り大きく4つのサイバーリスク分類体系が存在している[11](図表4)。

図表4 サイバーリスク分類体系の比較

分類体系の種類	主な分類基準／視点	フレームワークの例	利点	課題
攻撃手法による分類	どのような攻撃手法が用いられたか	MITRE ATT&CK、FBI IC3、PRC データセット	攻撃防止、脆弱性管理、社員教育に有効	技術用語が専門的すぎるため経営層・非技術者には理解しづらい、被害評価に不向き
損害／被害規模による分類	何がどれだけの損害を被ったか	保険会社が利用する枠組み（二重性分類を含む）	リスク定量化や被害金額の推計、保険商品開発に有効、非技術者にも理解しやすい	攻撃原因との因果関係はあいまいになりがち
オペレーショナルリスクによる分類	どのプロセスやシステム、組織要素が失敗したか	NIST SP800-30 ENISA Threat Landscape	業務影響評価や ERM との整合性が高い、既存リスク管理との接続が容易	攻撃技法や技術的背景が埋没しやすい、細分類が複雑になりがち
包括的アプローチ	総合的に何をどう評価するか	EU JRC による分類	政策立案や公的セクターでの包括的な情報把握に有効	ビジネス実務や保険、定量評価には不向き、過度な複雑性に陥る懸念あり

(出所)Rabittiら(2024)を参考に著者作成

図表4での比較の通り、現在提案されているサイバーリスク分類は、それぞれ異なる目的や背景に基づいており、必ずしも統一的ではない。サイバーセキュリティ実務者の中では MITRE ATT&CK などの「攻撃手法による分類」がよく利用されている。これはインシデントをトリガーとして原因特定から防御策改善までを実装する任務には非常に有用である。しかしながら、経営層や非技術者層にはハードルが高い内容となっているため、組織縦断・横断のコミュニケーションでの利用機会は少ないだろう。それと対照的なものが「損害／被害規模による分類」であり、本稿のメインテーマである「サイバーリスクの二重性」もこの分類に属する。この種の分類体系の利点は、シンプル

[11] Giovanni Rabitti, Amir Khorrami Chokami, Patrick Coyle, Ruben D. Cohen (2024) “A taxonomy of cyber risk taxonomies”

であることに尽きる。サイバーリスク理解におけるマクロ視点での合意や方向性を示したい場合に有効であるが、原因究明や因果関係の解読には適さない点には留意されたい。同じインシデントを繰り返さないための原因究明にはサイバー攻撃手法の特定が必須であるが、損害規模の推定には攻撃手法ではなく「何が侵害されるか」という資産の特定が重要変数なのである。

(2) 課題: サイバー損失データの標準化

サイバーリスク分類に関連する最重要課題は、サイバー損失データの標準化である。サイバー損失に関わる調査や報告はさまざまな主体から毎年報告されているが、悪意あるサイバー活動による被害規模を正確に把握するためのグローバルな統計基盤はいまだ発展途上であり、各国・各業界でのサイバーインシデントの分類や報告基準にはばらつきがある。そして、そのばらつきはサイバーリスク分類の標準化が為されていないことに起因する。「何をサイバー損害ひいてはサイバーイベントとして定義するか」に応じて観測対象が変わるからである。

サイバーリスク識別にどのような分類体系を用いるかの選択は、サイバー損失データの収集や解釈に大きな影響を与える。産官学にまたがるサイバーリスク領域の共通言語の確立は世界的な課題であり[12]、日本国内でもシンプルかつ実務的な分類体系の整備がサイバーセキュリティ分野の長期的な発展を支えていく基盤となる[13]。今後は機械学習や AI 技術を活用した「データ駆動型分類（data-driven taxonomy）」の活用も期待される。大規模なサイバーインシデントデータのクラスタリングによって、実態に即した新たな分類が導き出せる可能性もある。ただし、AI のアウトプットの質はインプットの質に依存するため、サイバーセキュリティ領域の長期的な成長は「サイバー損失データの標準化」という本質的問題の解決にかかっている。

5. 提言: 産官連携による「壊滅的リスクに対するサイバー保険体制の構築」

これまでの議論を包括し、日本のサイバーセキュリティの発展に向けて、筆者の私見を交えて 1 つの具体的な提案を述べたい。それは、「壊滅的リスクに対するサイバー保険体制の構築」が、これからのサイバーレジリエンス強化に向けた出発点になるという視座である。その理由は以下の二点である。

第一に、壊滅的リスク はもはや理論上の懸念ではなく、現実的な脅威であるという点である。発生頻度は低くともいったん起これば国家機能や社会基盤に甚大な影響を及ぼす可能性がある点において、サイバーイベントに起因する壊滅的リスクは地震とよく似た性質を持つ。地震と同様に「いつ起きるか」は予測困難である一方で、「いずれ起こる」ということは予見でき、社会として備えるべき対象であることは明白である。

第二に、サイバーリスクマネジメントにおいても、「地震対策の枠組み」が有効な示唆を与えるという点である。例えば、日本には地震保険制度とそれを支える政府による再保険制度[14]が存在しており、大規模災害時の経済的打撃に対して、民間と政府が連携して備える仕組みが整備されている。サイバー領域においても再保険に似た発想が求められる。つまり、産官学が共同して壊滅的リスクを前提としたサイバー保険制度を設計し、それを核としたサイバー保険市場を形成していくことが、社会全体のレジリエンスを新たな段階へと引き上げる。特に日本は、地震大国として大規模災害に対する経済的備えと制度設計に関して豊富な知見と経験を持つ。そして、それらの制度を支えるためにデータがいかに重要であるかも理解している。これをサイバー分野に応用することは、日本が国際的に貢献できる機会でもある。

---

[12] Vergara Cobos, Estefania; and Cakir, Selcen (2024) “A Review of the Economic Costs of Cyber Incidents” World Bank. Washington, DC

[13] この課題についての考察は別稿で改めて論じることとする。

[14] 財務省「地震保険制度の概要 – 政府による再保険」 https://www.mof.go.jp/policy/financial_system/earthquake_insurance/jisin.htm#2 (2025 年 6 月 26 日にアクセス)

6. まとめ:「サイバーセキュリティの失敗」の定義を変える

ここまで、サイバーリスク分類である「サイバーリスクの二重性モデル」について詳細に論じてきた。その締めくくりとして、「サイバーリスクの二重性モデル」によってもたらされる「サイバーセキュリティの失敗」に対する価値観の変容に注目したい。

従来、サイバーセキュリティの失敗は「インシデントが起こったか否か」で評価されていた。しかしながら、前述の通りサイバーインシデントは「いつか起きる」ものであるため、従来の基準は本質的に機能しない。サイバーインシデントの発生自体は好ましいことではないが、いつか「失敗」の烙印を押される日が来ることを分かっていながら日々の業務に情熱を燃やせる人間はいない。この構造が、サイバーセキュリティの現場に閉塞感をもたらしている。したがって、サイバーセキュリティの発展のためには従来の評価基準を変えなければならない。

筆者は、その変化をもたらし得るアプローチの１つが「サイバーリスクの二重性モデル」だと考える。現代のサイバー空間では消耗的リスクが日常的に発生し、それに対処すること自体が文字通り消耗を招く。さらには壊滅リスクという痛恨の一撃も発生し得る。このリスク分類に則ると、現代のサイバーセキュリティの失敗は、「『防御側が消耗しきった状態』または『壊滅的打撃から立ち直れない状態』になった場合」と定義できる。これこそが、現代のサイバーセキュリティの本質が「持続可能性（サステナビリティ）」や「レジリエンス」と表現される所以である。経済的・社会的・人的・技術的に持続可能なサイバーセキュリティの発展のために、本稿で取り上げた「サイバーリスクの二重性モデル」が浸透することを願って止まない。

石原　陽平　シニアアソシエイト

丸山　満彦　パートナー

PwC Intelligence
PwC コンサルティング合同会社

PwC Intelligence　統合知を提供するシンクタンク

https://www.pwc.com/jp/ja/services/consulting/intelligence.html

PwC コンサルティング合同会社

〒100-0004　東京都千代田区大手町 1-2-1 Otemachi One タワー　Tel：03-6257-0700