

〔論説〕

組織的サイバーハームの 多次元性と人間を中心とした解決策

The Multidimensional Nature of Organizational Cyber Harm and Human-Centered Solutions

蓮見 祥子

Sachiko HASUMI

要旨

本論説は、情報システム学会の掲げる「人間中心の情報システム」の理念に基づき、組織的サイバーハームを単なる技術的問題ではなく、人間・組織・社会の相互依存構造に根ざす多次元的現象として再定義するものである。従来のサイバーセキュリティは、機密性・完全性・可用性（CIA）を軸とした技術的防御に重点を置いてきたが、近年のインシデントは、人的・心理的・経済的・社会的影響を連鎖的に拡大させる複合的なサイバーハームとして顕在化している。本論説は、既存研究の批判的統合および日本事例の分析を通じて、サイバーハームの伝播構造、危機過程、および認知・関係・感情の三側面からなる中核構造を提示する。その上で、技術中心の防御モデルの限界を指摘し、人間の判断・行動・心理的回復を中核に据えた人間中心サイバーレジリエンスへの転換の必要性を論じる。さらに、インフラ層、ビジネスプロセス層、人間・文化層の三層構造に即して設計原則と実装戦略を提示し、実務および政策への応用可能性を示す。

Abstract

This paper, grounded in the principle of human-centered information systems, redefines organizational cyber harm as a multidimensional phenomenon embedded in interdependent socio-technical structures across infrastructure, business processes, and human-cultural dynamics. Traditional cybersecurity has emphasized technical controls based on the CIA triad; however, recent incidents reveal cascading harm that extend beyond technical disruption to psychological, relational, economic, and societal domains. Through a critical synthesis of prior research and an analysis of Japanese cases, this paper identifies the propagation structure of cyber harm, the crisis process through which organizations experience it, and its core internal dimensions: cognitive, relational, and emotional. On this basis, the paper argues that technology-centered defense models are insufficient on their own and that a shift toward human-centered cyber resilience is necessary, with greater emphasis on human judgment, behavior, trust, and recovery. It then proposes design principles and implementation strategies aligned with the three layers of infrastructure, business processes, and human-cultural dynamics and discusses their implications for organizational practice and public policy.

1. はじめに

1.1. 本論説の目的

本論説は、情報システム学会が掲げる「人間中心の情報システム」の理念に立脚し、組織的サイバーハーム（以下、サイバーハーム）という現代的課題を、単なる技術的問題としてではなく、人間・組織・社会の相互依存構造に根ざす制度的・文化的問題として再定位することを目的とする。あわせて本論説は、実証研究の報告ではなく、既存研究の批判的統合および日本における事例分析を通じて理論的含意と実務的示唆を提示する立場表明型論考として位置づけられる。

本論説の主眼は、従来の技術・プロセス中心の防御モデルを批判的に再検討し、サイバーハームの多次元的理解に基づく人間中心の解決枠組みを提示することにある。従来のサイバーセキュリティは、機密性・完全性・可用性（CIA: Confidentiality, Integrity, Availability）を基軸として、技術的防御および統制の最適化を中心に発展してきた。しかしながら、近年のサイバーインシデントは、単なる技術的障害として把握するには不十分であり、組織内外の相互依存関係を通じて影響を連鎖的に拡大させ、人的・経済的・社会的側面において複合的な被害、すなわちサイバーハームを生起させる現象として顕在化している。

〔論説〕

2026 年 3 月 25 日受付, 2026 年 4 月 30 日受理

© 情報システム学会

この問題意識に基づき、本論説は三つの論点を提示する。第一に、サイバーインシデントは単一の技術的事象として完結するものではなく、組織の内部および外部にまたがる複雑な相互依存構造の中で連鎖的に増幅される現象として理解されるべきであることを明らかにする。第二に、この再定義を踏まえ、従来の技術中心のサイバーレジリエンス概念を相対化し、人間の判断・行動・心理的回復を中核に据えた人間中心アプローチへの理論的転換の必要性を論じる。第三に、サイバーハームに対応する具体的方策として、インフラ層、ビジネスプロセス層、人間・文化層の三層構造に即した設計原則および実装戦略を提示し、その実務的・政策的含意を示す。

以上を通じて本論説は、サイバーセキュリティを技術的防御の問題として狭く把握する従来の視座を批判的に再検討し、サイバーハームに対する理解と対応の基盤を、「人間中心の情報システム」という観点から再構築することを目的とするものである。

1.2. 組織的サイバーハームの定義

Agrafiotis らのサイバーハーム分類枠組み[1]と, Lindsey と Glasser によるハーム測定方法論[2]を理論的基盤として、本論説では組織的サイバーハームを、サイバーインシデントを契機として組織の内部または外部に生起し、組織の業務遂行、資産、意思決定、対外的関係、ならびに取引先・利用者・社会基盤にまで波及しうる実際的または潜在的な有害影響の総体として操作的に定義する。ここでいうハームは、単なる情報システム上の障害や情報資産の侵害に限定されず、物理的・デジタル的、経済的、心理的、評判的、社会的・社会制度的影響を含む多次元的現象として理解される[2][3]。

この定義の意義は、従来のサイバーセキュリティ研究が主として依拠してきた機密性・完全性・可用性（CIA）中心の保護対象論から、侵害後にいかなる悪影響が、誰に、どの範囲まで及ぶのかという影響分析へと視点を移す点にある。Agrafiotis らは、組織が被るサイバーハームを五つの大分類の下に整理するとともに、それらのハームが相互に関連し、時間の経過とともに伝播しうることを示した[1]。また、Lindsey と Glasser の方法論は、復旧時間、直接費用、漏えい件数といった限定的指標のみでは被害の実像を把握できず、人、組織、社会、さらには平和・安全保障への影響までを含めて把握する必要があることを指摘している[2][3]。

したがって、組織的サイバーハームには、システム停止や情報漏えいのような直接的被害のみならず、意思決定の停滞、従業員や関係者への心理的負荷、顧客・取引先との関係悪化、規制対応や法的責任への対処負担、さらには社会的信頼の低下といった二次的・三次的影響も含まれる。とりわけ経済的影響については、Romanosky がサイバーインシデントの費用分析を通じてその把握の重要性を示す一方、公開データに基づく費用推計は、逸失収益、市場価値の変動、消費者側被害、社会的外部性等を十分に含まないことも示している。これは、サイバーハームを単一の財務指標へ還元することの限界を示すものであり、被害把握においては複合的視点が不可欠であることを意味する[3]。

さらに、日本の組織実務においては、サイバーセキュリティは情報処理部門の技術課題ではなく経営課題として位置づけられており、経営層の関与、責任分担の明確化、セキュリティ責任者等を含む統治構造、ならびにインシデント対応体制の整備が重視されている。経済産業省の「サイバーセキュリティ経営ガイドライン Ver 3.0」は、経営陣が主体的に組織体制と資源配分を担うべきことを明示しており、組織的サイバーハームを理解するうえで、被害は技術層だけでなく統治・判断・説明責任の層にも現れることを示唆する[4]。

加えて、日本政府のサイバーセキュリティ政策文書は、サイバー攻撃の影響が標的組織にとどまらず、サプライチェーン全体や重要インフラの機能維持にまで及ぶことを明確に指摘している。実際、取引先を踏み台とした攻撃や、医療機関・港湾等の停止事案が示すように、組織に生じたハームは、顧客、委託先、地域社会、社会基盤へと拡張しうる。ゆえに、組織的サイバーハームは、個別組織に閉じた損害概念ではなく、相互依存的な社会システムの中で連鎖・増幅する現象として把握されなければならない[5]。

以上より、本論説は、組織的サイバーハームをサイバーインシデントによって発生し、組織内部の業務・統治・意思決定から、対外的関係、経済的損失、社会的信頼、社会基盤の機能にまで波及しうる多層的・伝播的な有害影響として捉える。この定義は、サイバーセキュリティを「侵害を防ぐ技術」の問題としてのみではなく、「侵害後に何が壊れ、どのように広がるのか」を分析するための概念装置として位置づけるものである[2][3][5]。

2. 組織的サイバーハームの多次元性

本章では、既存の学術理論および事例研究の検討を通じて、サイバー事案を単一の技術的出来事とし

て把握する従来の見方を再検討する。Cains らが示すように、サイバーセキュリティおよびサイバー上の危険は、本質的に技術、組織、人間行動、制度環境を横断する学際的対象である[6]。この観点に立てば、サイバー事案は、情報資産や情報システムへの侵害にとどまらず、組織の内部および外部にまたがる相互依存的構造のなかで連鎖的に増幅されるサイバーハームとして理解されるべきである。

本章の目的は、サイバーハームがどのように広がり、組織内部でどのような危機過程をとり、何が中核的に損なわれるのかを理論的に整理することにある。具体的には、2.1 では「被害がどこへ広がるか」という伝播構造、2.2 では「組織がどのように危機を経験するか」という危機過程、2.3 では「内部で何が壊れるか」という中核構造を明らかにし、2.4 で二つの事例を用いてその妥当性を検討する。

2.1. サイバーハームの伝播構造理論

Agrafiotis らの研究は、サイバーハームを単発的な被害ではなく、相互に連結した資産、業務、主体、社会的関係を通じて段階的に拡大しうる現象として捉えている[1]。本節ではこの視点を踏まえ、サイバーハームの伝播構造を、初期事案、組織内部への伝播、組織外部への伝播、二次的・長期的被害の四段階として整理する。重要なのは、サイバー攻撃の影響が技術的障害として発生したのち、組織機能、対外関係、社会的信頼へと連鎖的に広がりうる点にある[1][2]。

第一段階は、初期事案である。たとえば、身代金要求型不正プログラムによる暗号化、情報漏えい、認証基盤の侵害、重要システムの停止などがこれに当たる。この段階では、影響は情報資産や情報システムに集中しているように見える。しかし Agrafiotis らが示すように、こうした被害はそれ自体で完結するのではなく、その後に生じる複数の被害の起点となる[1]。

したがって、初期事案は単なる技術的障害ではなく、後続する組織的・社会的被害を引き起こす出発点として理解されなければならない。また、経済産業省の指針および米国国立標準技術研究所の文書が示すように、この段階からすでに、当該事案は情報部門だけの問題ではなく、経営上の危機として把握されるべきである[4][7][8]。

第二段階は、組織内部への伝播である。初期侵害が発生すると、その影響は業務手順、意思決定、顧客対応、復旧判断、資源配分へと波及する。被害評価は復旧時間や直接費用だけに限定されるべきではなく、組織の機能維持、人員、業務継続性を含む多面的影響として把握される必要がある[2]。また、経済産業省は、サイバーセキュリティを経営課題と位置づけ、経営層の関与、責任分担の明確化、対応体制の整備を求めている[4]。さらに、米国国立標準技術研究所は、サイバー上の危険を組織全体の危険として整理し、下位の技術情報を上位の経営判断へ接続することの重要性を示している[8]。このように、内部伝播とは、システム障害が業務停止、判断遅延、対応負荷の増大へと転化し、組織機能そのものを損なっていく過程である。加えて、Weick が示したように、危機的状況では「何が起きているのか」を組織として理解し、行為の意味を再構成する営みが崩れること自体が被害を深めうるため、内部伝播は技術的障害の拡大であると同時に、組織的意味づけの崩れでもある[9]。

第三段階は、組織外部への伝播である。サイバーハームは組織内部にとどまらず、顧客、委託先、取引先、さらには社会基盤へと広がりうる。日本の政策文書は、供給網を介した攻撃や重要基盤停止の事例を通じて、被害が標的組織を超えて広がりうることを示している[5]。また、Barrot と Sauvagnat は、生産ネットワークにおいて、代替の難しい投入を担う企業に生じた衝撃が取引先へ有意に伝播することを示しており、この知見は供給網を通じたサイバーハームの広がりを理解するうえで有益である[10]。加えて、欧州連合サイバーセキュリティ機関は、サイバーセキュリティを単なる技術統制ではなく、人間の行動、組織文化、社会的相互作用を含む問題として捉える必要があると指摘している[11]。この段階では、被害はもはや一組織の内部問題ではなく、相互依存的な関係のなかで広がる社会的問題へと変質する。

第四段階は、二次的・長期的被害である。事案の公表、説明、復旧、再発防止の過程では、規制対応費用、訴訟危険、評判の毀損、顧客離れ、取引関係の悪化、社会的信頼の低下といった影響が生じうる。Romanosky は、サイバー事案の費用分析において、公表データから把握できる損失は全体の一部にすぎず、逸失収益や社会的波及損失を十分に含まないことを示している[3]。また、Gwebu らは、情報漏えい後の企業評価や企業価値の維持において、事後対応のあり方が大きな意味をもつことを示している[12]。さらに、Kuipers と Schonheit は、危機時の広報において、否認は評判回復に不利であり、責任の受容、詳細な説明、補償、是正措置を一貫して提示することが被害の軽減に資することを示している[13]。したがって、二次的被害とは、侵害そのものの結果であるだけでなく、その後の説明責任や対応の仕方によって増幅も緩和もされうる動的な被害領域である。

さらに、二次的・長期的被害は、従業員や関係者に対する人的・組織的影響としても現れる。Islam ら

は、サイバーハームの管理において、測定の困難さ、人的要因、責任の重複、訓練不足、制度的欠陥が重要な課題であることを示している[7]。このことは、被害の持続化が個人の問題ではなく、組織設計や実務体制の問題とも結びついていることを示唆する。また、Litz らのいう道徳的損傷は、本来は戦争経験における心理的損傷を説明する概念であるため、サイバー分野への適用には慎重が必要であるが、「防げなかった」「適切に対処できなかった」という認識が強い罪責感や心理的負荷をもたらしていることを考える補助線としては有用である[14]。同様に、Smith と Freyd の制度的裏切りという概念は、組織が本来果たすべき保護や対応を怠ったときに、構成員の不信感や心理的苦痛が増幅される過程を説明するうえで有効である[15]。加えて、欧州連合サイバーセキュリティ機関が示すように、サイバーセキュリティ文化は単なる規則の遵守ではなく、信頼、価値観、行動、組織的実践の総体として形成されるため、事後対応が過度の統制や一方的な責任追及に傾く場合、それ自体が新たな被害を生み出しうる[11]。

この点で重要なのは、組織が危機ののちに単に元の状態へ戻れるかどうかではなく、負荷が増大するなかでも適応能力を維持し、必要に応じて拡張できるかどうかである。Woods は、回復力を単なる原状復帰ではなく、予期しない事態に直面したときに脆さを露呈させず適応能力を発揮する性質として捉えている[16]。この見方に立てば、組織的サイバーハームの本質は、被害の発生それ自体にあるだけでなく、被害後の組織がどこまで持ちこたえ、学び、関係を修復しうるかという点にもある。

以上より、組織的サイバーハームの伝播は、技術的侵害から始まり、組織内部の業務と統治へ波及し、さらに供給網、顧客、社会基盤へと拡張し、その後も制度、評判、心理、組織文化の次元で持続する多層的過程として理解されるべきである[1][2][5][8][11]。本章における伝播構造型論の意義は、サイバー事案を単発の事故としてではなく、時間的・関係的に展開する複合的被害の生成過程として捉え、その抑制と回復の条件を組織レベルで検討可能にする点にある[9][12][13][16]。

2.2. Caplan の危機理論による組織的分析

前節では、サイバーハームがどのように段階的に伝播するかを示した。これに対し本節では、その伝播過程が組織内部ではどのような危機過程として経験されるのかを検討する。そのための理論的基盤となるのが、Caplan の危機理論である[17]。

Caplan の危機理論は、本来、個人が平常時の対処能力では処理しきれない事態に直面したとき、緊張の増大を経て危機状態へ移行する過程を説明するものである[17]。この理論は個人心理を対象として構想されたものであるが、危機が既存の均衡を崩し、通常の実行様式を無効化し、外部資源の動員や新たな適応を要請するという点において、組織にも応用可能である。とりわけ Fink らは、危機への人間的適応過程を組織危機の説明へ拡張し、組織が危機の進行に伴って段階的変化をたどることを示している[18]。本節ではこの理論的系譜を踏まえ、サイバー事案発生時の組織的危機過程を、衝撃、拡大、動員、適応または崩壊の四段階として整理する。

第一段階である衝撃では、侵害が検知され、標準作業手順や初動対応手順が起動される。この段階では、組織はなお既存の規則と役割分担によって状況を制御できると想定している。しかし、危機理論の観点から見れば、この時点ですでに従来の均衡は動揺しており、平常時の処理能力が試され始めている[17][18]。

第二段階は、拡大である。ここでは、標準作業手順が十分に機能しないことが明らかとなり、被害が業務停止、混乱、対応遅延として広がる。たとえば、予備系統も侵害されていた場合や、復旧手順自体が現実に適合しない場合、組織は予定していた制御モデルを維持できなくなる。この段階は、危機理論における従来の対処様式の失効に相当し、組織が「手順どおりに動いているにもかかわらず、事態を抑えられない」という転換点である[17][18]。したがって、この局面は単なる被害拡大ではなく、既存の統制構造の限界が露呈する局面として理解される。

第三段階は、動員である。組織は、法務、広報、外部調査、復旧支援、監督当局対応などのために外部資源を投入し、内部の人的・時間的資源を再配分する。この段階では、危機への対応が情報部門の作業を超え、組織全体の総動員体制へ移行する。すなわち、危機はもはや局所的障害ではなく、経営判断、説明責任、対外関係を巻き込む組織全体の課題となる[4][8]。動員の拡大は、危機への適応努力であると同時に、組織の余力の消耗過程でもある。

第四段階は、適応または崩壊である。危機への対応を通じて新たな手順、役割分担、関係調整が確立されれば、組織は均衡を再構築し、一定の学習と回復に至る。他方、対応の失敗や説明責任の不履行が続けば、評判の毀損、人材流出、顧客離れ、内部不信の固定化といった形で、危機は長期的損傷へと転化する[12][13][16]。この意味で、危機過程の終点は単なる技術的復旧ではなく、組織が新たな均衡を形成できたか、それとも傷ついたまま脆弱化したかによって区別される[16][18]。

以上より、サイバー事案への組織的対応は、単なる技術復旧の手順ではなく、組織の均衡が崩れ、資源が再配分され、最終的に再構築または脆弱化へ至る危機過程として理解されるべきである。特に第二段階における標準作業手順の破綻は、従来の統制モデルの限界が露呈する決定的な転換点であり、ここに組織的サイバーハームの深まりを見ることができる[17][18]。

2.3. 組織的サイバーハームの中核構造理論

前二節では、サイバーハームが時間の経過とともに伝播し、また組織危機として展開する過程を示した。本節ではさらに一步進めて、そうした被害が組織内部でどのような構造をとって現れるのかを明らかにする。ここで鍵となるのは、サイバーハームが単なる情報資産の損傷ではなく、第1層のインフラ層、第2層のビジネスプロセス層、第3層の人間・文化層にまたがって、とりわけ組織内部では認知、関係、感情という三つの中核領域において顕在化する複合的現象であるという点である[1]。

第一に、認知的ハームがある。これは、組織が状況を把握し、判断し、行為を調整するための認識基盤が損なわれる被害である。データの消失や改ざん、監視情報の欠落、記録の破損などは、組織の制度的記憶と判断基盤を毀損し、意思決定の質と速度を著しく低下させる[1]。さらに、Weick が示したように、危機下では「何が起きているのか」を組織として理解する意味づけの営み自体が崩れうるため、被害は単なる情報不足ではなく、組織的認識能力の崩壊として現れる[9]。この意味で認知的ハームとは、事実の欠落だけではなく、状況理解の枠組みそのものが失われることを含む。

第二に、関係的ハームがある。これは、経営層、従業員、顧客、取引先、監督機関などを結んでいた信頼と役割期待が傷つく被害である。特に、組織が本来果たすべき保護責任や説明責任を果たしていなかったと認識された場合、その不信は単なる失望ではなく、Smith と Freyd のいう制度的裏切りとして経験されうる[15]。制度的裏切りは、組織への依存や信頼を前提としていた構成員ほど深く経験されやすく、危機後の協力、忠誠、帰属意識を大きく損なう[15]。したがって、関係的ハームは、被害後の説明不足、責任転嫁、支援欠如などを通じて増幅され、組織の結束を内部から弱体化させる。

第三に、感情的ハームがある。サイバー事案への対応過程では、緊張、不安、恐怖、怒り、羞恥、非難といった感情が組織内に広がりやすい。とりわけ、対応責任を負う担当者が「防げなかった」「適切に対処できなかった」と認識する場合、その心理的負荷は強い罪責感や自己否定へと結びつきうる。この点で、Litz らのいう道徳的損傷は、本来は戦争経験に関する概念であるため直接適用には慎重さを要するものの、重大な失敗をめぐる深い心理的傷つきを考える補助線として有用である[14]。また、Cram らが示すように、情報セキュリティに関する要求や負荷が過度に蓄積すると、構成員には情報セキュリティ疲労が生じ、それが遵守行動や態度に影響を及ぼしうる[19]。したがって、感情的ハームは一時的な緊張ではなく、疲弊、冷笑、責任回避、相互非難といった形で組織機能を低下させる可能性がある。

これら三つの内部的ハームは、それぞれ独立して存在するのではなく、相互に作用しながら組織の基盤を崩していく。認知的混乱は関係的不信を強め、不信は感情的緊張を増幅させ、感情的対立はさらに判断の質を低下させる。この循環が進行すると、組織は事案そのものへの対応だけでなく、内部の混乱そのものの管理に追われるようになる[1][9][19]。さらに、これらの内部的ハームは外部へも波及する。Agrafiotis らの分類が示すように、組織的サイバーハームは、経済的損失、評判の毀損、心理的影響、物理的・情動的被害、社会的・制度的影響という複数の次元で現れる[1]。内部における認知、関係、感情の崩れは、やがて顧客対応の失敗、広報の不整合、取引関係の悪化、社会的信頼の低下へと外在化し、組織外部に可視化される被害を生み出す[12][13]。

重要なのは、これらのハームが単純に並列しているのではなく、認知の崩れが関係の崩れを招き、関係の崩れが感情の混乱を増幅し、その結果が経済的・社会的被害へ波及するという連鎖構造をなしている点である。この意味で、組織的サイバーハームとは、サイバー事案を契機として人間の判断、信頼、感情が損なわれ、その損傷が組織内外へ拡張していく複合的被害の生成過程である[1][9][15][19]。したがって、組織的サイバーハームの中核構造を理解するためには、技術的侵害だけでなく、認知、関係、感情の三領域における損傷とその相互作用を分析の中心に据える必要がある。

3. ケーススタディ：サイバーハームの多次元的発現

本節では、前節までに理論的に整理した組織的サイバーハームの多次元性について、実際の事例を用いてその発現過程および影響の具体的様態を検証する。ここでは、組織内部の機能不全、対外的な影響の拡大、説明責任と回復の問題が比較的明確に観察できる二事例として、アサヒグループホールディングス事案とアスクル事案を取り上げる。

3.1. アサヒグループホールディングスへのサイバー攻撃

アサヒグループホールディングスは、2025 年 9 月 29 日、サイバー攻撃に起因するシステム障害の発生を公表した。同社によれば、日本国内の受注・出荷業務およびコールセンター業務が停止し、影響は国内運用に限定されたものの、事業継続に直接的な支障が生じた[20]。その後の調査結果では、攻撃者がグループ拠点にあるネットワーク機器を経由してデータセンターのネットワークへ侵入し、ランサムウェアを一斉実行した結果、複数のサーバーおよび一部のパソコン端末のデータが暗号化されたことが明らかにされた[21]。

この事例は、多次元的ハームの発現を比較的明確に示している。第一に、認知的ハームとして、サーバーや端末の暗号化は、業務遂行に必要な情報へのアクセス可能性を損ない、状況把握、判断、調整の基盤を弱体化させる。第二に、関係的ハームとして、顧客対応窓口や出荷機能の停止は、顧客や取引先との接点に直接影響を及ぼし、説明責任への圧力を高める。さらに、調査結果では、合計 191 万 4 千件の個人情報について流出の可能性が示されており、内訳には顧客相談室利用者、社外関係先、従業員およびその家族が含まれている[21]。これは、被害が企業内部の情報障害にとどまらず、広範な利害関係者との信頼関係に関わる問題へ転化したことを意味する。

また、この事例は伝播構造の観点からも典型的である。初期事案はネットワーク侵入とランサムウェア実行という技術的侵害であったが、それはただちに受注・出荷・顧客対応機能の停止へと内部伝播し、その後、個人情報流出可能性の公表を通じて対外的な信頼問題へと外部化した[20][21]。さらに、再発防止策として、通信経路およびネットワーク制御の再設計、外部接続の安全領域への限定、監視体制の見直し、攻撃を想定したバックアップ戦略と事業継続計画の再設計、社員教育と外部監査の強化が示されている[21]。このことは、被害後の課題が単なる技術復旧ではなく、統治、監視、学習、事業継続の再構築へ及んでいることを示している。

したがって、アサヒグループホールディングス事案は、サイバー事案が情報システム障害として始まりながら、業務継続、顧客接点、個人情報保護、組織統治、回復力の問題へ連鎖的に拡大することを示す事例である。ここでは、2. 1 節で示した伝播構造と、2. 2 節で論じた危機過程とが重なり合い、組織的サイバーハームの多層性が具体的に確認できる[1][8][16]。

3.2. アスクル株式会社へのサイバー攻撃

アスクル株式会社は、2025 年 10 月 19 日、外部からの不正アクセスによりランサムウェアに感染し、サービスが一時停止するとともに、顧客情報および一部取引先情報が外部へ流出したことを公表した[22]。同社の調査結果によれば、攻撃者は認証情報を窃取して不正利用し、例外的に多要素認証が適用されていなかった業務委託先向け管理者アカウントを侵入口として、ネットワーク内部に侵入した[23]。侵入後、攻撃者は複数のサーバーへ移動し、脆弱性対策ソフトを無効化したうえで権限を拡大し、複数種のランサムウェアを用いてデータ暗号化とバックアップ削除を行ったことが明らかにされている[23]。

この事例において特徴的なのは、高度に自動化された物流システムへの依存が、被害の組織的拡大を加速させた点である。アスクルは、物流センターの自動倉庫設備やピッキングシステムを含む物流システムの停止によって、出荷業務を全面停止する重大な影響を受けた[23]。このことは、認知的ハームが単なる情報アクセス障害にとどまらず、「どこまで安全か」「何を再開できるか」という基準そのものの喪失として現れたことを意味する。さらに、調査結果では、事業所向けサービス、個人向けサービス、取引先、役員・社員等を含む計 73 万 9700 件の情報が影響を受けたとされており[23]、関係的ハームも広範囲に及んだことが分かる。

また、この事例は、供給網的依存と回復過程の問題を示すうえでも重要である。初期侵入は一つの管理者アカウントから始まっているが、その影響は自社内部のシステム停止にとどまらず、物流機能全体の停止という形で事業継続能力を損なった[22][23]。加えて、同社は攻撃検知後、感染疑いシステムの分離、認証情報のリセット、管理者アカウントへの多要素認証適用、監視体制の強化などを段階的に実施し、11 月には安全性確認を踏まえて一部の注文機能を再開した[22]。さらに、再発防止策として、全ての遠隔接続への多要素認証の徹底、管理者権限の厳格運用、24 時間 365 日の監視体制、多層的検知体制、ランサムウェアを想定したバックアップ環境の整備が示されている[23]。

このように、アスクル事案は、供給網と自動化への依存が高い組織において、認証統制の例外運用がいかに大きな組織的被害へ結びつくかを示している。同時に、バックアップ削除や長期復旧の問題は、サイバー事案が単発の障害ではなく、危機過程と回復力の問題として理解されるべきであることを明確にしている[8][16][23]。

3.3. 小括

以上の二事例は、組織的サイバーハームが、技術的侵害から始まり、組織内部の機能停止、利害関係者との関係悪化、情報流出、回復過程の長期化へと連鎖することを具体的に示している。アサヒグループホールディングス事案では、受注・出荷・顧客対応の停止と大規模な個人情報流出可能性が、説明責任と信頼維持の問題を前景化させた[20][21]。これに対しアスクル事案では、認証運用の例外が初期侵入を許し、高度に自動化された物流基盤の停止とバックアップ削除によって、回復困難性が一層顕著になった[22][23]。

両事例に共通するのは、被害が技術的領域に閉じず、認知、関係、感情、評判、統治、事業継続といった複数の領域へ拡張している点である。このことは、サイバー事案を単なる情報資産侵害としてではなく、組織の均衡、信頼、回復力を揺るがす多次元的危機として把握する必要性を裏づけている[1][2][12][13][16]。したがって、ケーススタディの検討は、前節までに示した理論枠組みが、実際の組織事案に対して十分な説明力を有することを示すものである。

4. 人間中心のサイバーレジリエンスへのパラダイムシフトの必要性

本章では、前章で示した組織的サイバーハームの構造分析を踏まえ、従来の技術中心型サイバーセキュリティの限界を検討し、人間中心サイバーレジリエンスへの理論的転換の必要性を論じる。特に、本章では、組織的サイバーハームがインフラ層、ビジネスプロセス層、人間・文化層へと多層的に広がる点に着目し、それぞれに対する理論的対応可能性を整理する。

4.1. 理論的根拠

本節では、まず、なぜ技術的アプローチのみではサイバーハームへの対応が構造的に不十分であるかを論じ、次いで三層構造に沿って人間中心アプローチの必要性を整理する。Anderson らが示したサイバー犯罪コストの体系的視点を踏まえると、サイバーハームは単なる技術的障害ではなく、組織内外の相互依存構造の中で連鎖的に拡大する構造的現象として理解されるべきである[24]。また、Cains らが示すように、サイバーセキュリティおよびサイバー上の危険は、技術・組織・人的行動・制度環境を横断する学際的対象であり、単一の技術統制だけでは十分に把握できない[6]。

この意味で、サイバー事案は組織の均衡を崩壊させると同時に、従業員、顧客、取引先、社会基盤の利用者を含む多様な主体に有害影響を及ぼす。したがって、サイバーセキュリティは従来の防御技術としてではなく、ハームの伝播を抑制し、組織の均衡を維持し、人の回復を支える設計として再定義される必要がある[16][25][26][27]。

本節では、サイバーハームを以下の三層構造として整理する。

表 1 サイバーハームの三層構造

層	名称	主な内容
第1層	インフラ層	システム障害、データ損失、サービス停止
第2層	ビジネスプロセス層	業務中断、供給網混乱、財務的損失
第3層	人間・文化層	信頼崩壊、心理的負荷、制度的裏切り、組織文化の毀損

この三層構造において、第1層は技術的基盤の損傷、第2層は組織活動の継続性への影響、第3層は信頼、感情、文化、制度的整合性への影響を示す。とりわけ第3層の人間・文化層におけるハームは、長期的な組織の衰退をもたらす中核的影響であり、従来の技術中心の枠組みでは十分に扱われてこなかった領域である[7][11][15]。

CIA 原則を中心とする防御モデルは、侵害の予防や影響局所化には有効であるが、ハームが顕在化した後にいかに吸収し、回復し、適応するかという問題に対しては構造的に不十分である[8][25]。むしろ必要なのは、被害の有無だけではなく、被害後にどこまで機能を維持し、どのように関係と判断能力を回復できるかに着目するサイバーレジリエンスへの移行である[16][25]。

もっとも、技術的防御の高度化それ自体を否定すべきではない。ゼロトラスト、多層防御、認証強化、監視高度化などは依然として不可欠である[8]。しかし、本章が問題にするのは、それらの有効性ではなく、その適用範囲の限界である。アサヒグループホールディングス事案およびアスクル事案が示すように、侵害の検知や封じ込めに着手した後であっても、判断遅延、信頼の揺らぎ、説明責任への圧力、組織文化の疲弊といったハームは進行し続けた[20][21][22][23]。この意味で、人間中心アプローチは技術的防御の代替ではなく、それでは補えない次元のハームに対処するための補完的かつ必要条件的な枠組みとして位置づけられる。

4.2. 三層構造に対応した理論的対応

4.1 で示した三層構造に照らすと、人間中心アプローチは各層に対して異なる理論的対応を必要とする。以下では、第1層のインフラ層、第2層のビジネスプロセス層、第3層の人間・文化層に即して、その理論的基盤を整理する。

第一に、第1層のインフラ層に対しては、技術的防御の強化が依然として不可欠である。ただし、人間中心アプローチが付加する論点は、インフラの損傷を単なる停止としてではなく、その後の判断と行動の条件を左右する基盤損傷として捉える点にある。すなわち、重要なのは、システムが損なわれた際にも、組織が何を把握し、どこまで安全に動けるかを維持できるようにすることである。この意味で、第1層における人間中心性とは、技術的冗長化に加えて、状況把握しやすい可視化、優先順位づけ、代替手順への移行可能性を設計することにある[8][16][25]。

第二に、第2層のビジネスプロセス層に対しては、認知的ハームへの対応が中核となる。ここで問題となるのは、制度的記憶の喪失と意思決定麻痺である[1][9]。これに対する理論的根拠として有力なのが、取引記憶システムである。取引記憶システムとは、「誰が何を知っているか」を組織内で共有する分散的知識構造を指し、集団が個々人の知識を相互補完しながら全体として判断能力を維持する仕組みである[28][29]。この観点からみれば、サイバー事案時に必要なのは、データが欠けても、誰が代替判断を担えるか、どの部門が何を補完できるかが分かる状態を保つことである。ここでいう分散型知能とは、複数の担当者・部門・外部支援主体が、部分的知識を相互補完しながら全体として行動能力を維持する状態を意味する。したがって、人間中心の対応とは、知識冗長性の文化を構築し、訓練や演習を通じて、「データが欠けても判断できる組織」を設計することにある。

第三に、第3層の人間・文化層に対しては、関係的ハームおよび感情的ハームへの対応が中核となる。関係的ハームの問題は、信頼の崩壊と、組織が注意義務や説明責任を果たさなかったという認識である[12][13][15]。この領域では、組織正義理論が有力な根拠を与える。Greenberg は、組織における公正の知覚が従業員の受容、納得、信頼を左右すると論じ[30]、Colquitt は分配的公正、手続的公正、対人的公正、情報的公正という多次元の把握を提示した[31]。さらに、Colquitt らのメタ分析は、公正知覚が信頼、職務態度、組織市民行動と広く結びついていることを示している[32]。この視点からすれば、人間中心の対応とは、コンプライアンス中心の統制のみを強化するのではなく、透明性、公正性、一貫性、説明責任を通じて心理的契約を維持することである。

また、第3層では感情的ハームと心理的影響への対応も重要である。問題となるのは、高ストレス環境における恐怖、責任追及、疲弊の連鎖である[7][14][19]。ここで中核的となるのは、レジリエンス工学の視点である。Hollnagel は、従来の「失敗を減らす」安全管理から、変化の中で機能を維持し適応する能力を重視する考え方への転換を提起した[25]。Woods も、回復力を単なる反発的復旧ではなく、負荷の高まりに対して機能を拡張しうる能力として捉えている[16]。これに照らせば、人間中心の対応とは、インシデント対応チームへの心理的支援、感情的負荷の可視化、危機時の対話的コミュニケーションを導入し、感情的伝染が組織崩壊へと連鎖することを防ぐことである。

以上のように、第1層では基盤損傷下でも行動可能性を維持する設計、第2層では取引記憶システムと分散型知能によって判断停止を回避する設計、第3層では公正性、信頼、心理的安全性を支える設計が求められる。したがって、人間中心サイバーレジリエンスとは、三層構造の各層に異なる仕方で介入しながら、サイバーハームの連鎖を抑制する統合的枠組みである。

4.3 パラダイムシフトの骨格：技術防御から人間中心レジリエンスへ

前節で示した三層構造ごとの理論的対応を踏まえると、パラダイムシフトの骨格は、技術防御を否定することではなく、それを人間の判断、信頼、学習、回復を支える設計へと埋め込むことにある。

人間中心のサイバーセキュリティが多次元のサイバーハームをどのように緩和するかを理解するためには、社会技術システム論の視点が不可欠である。社会技術システム論は、組織を「人・プロセス・技術」が相互依存する統合的システムとして捉え、この相互作用の設計によって危険の伝播連鎖を制御できることを示している[11][26]。この視点に立てば、サイバー事案への対応は、境界防御の問題であるだけでなく、判断、信頼、行動、学習、回復を含む組織設計の問題である。

この枠組みにおいて、人間中心サイバーレジリエンスは、ハームの発生後に対処するだけでなく、各段階において伝播の連鎖を断ち切ることを目的とする。その中核となるのが、判断のための時間的余裕、報告のための心理的安全性、説明のための制度的整合性、そして回復のための学習能力である[16][25][30][31]。言い換えれば、サイバーセキュリティは、侵害を一件も起こさないことだけで評価されるのではなく、侵害後にどこまで壊れず、どこまで戻れ、どこまで学べるかによって再評価されるべ

き段階に来ているのである。

表 2 パラダイムシフトの骨格

観点	従来の技術的防御	人間中心サイバーレジリエンス
目的	不正侵入・不正操作の防止	組織の継続性と回復の確保
人間観	管理すべき脆弱性	能動的な防御主体・回復資産
主な評価指標	復旧時間, 停止時間, 侵入件数	判断回復, 信頼回復, 安定回復の速度と質
事後対応	技術的修復	学習, 関係修復, 文化的適応
統治の焦点	システム統制	社会技術的整合性

5. 組織的サイバーハームへの人間中心解決策：設計原則と実装戦略

本章では、前章までで示した組織的サイバーハームの多次元構造および人間中心サイバーレジリエンスの必要性を踏まえ、それを組織へ実装するための設計原則および具体戦略を提示する。ここで示す内容は、単なる技術的統制の追加ではなく、人間の判断、信頼、心理的回復、学習能力を含む社会技術的システム全体を再設計するための実装枠組みとして位置づけられる。

5.1. 設計原則：三つの中核的方針

人間中心アプローチの設計原則は、第2章で分析した三つの中核的被害領域に対応して、以下の三点に集約される。

表 3 人間中心設計原則と中核的被害領域

設計原則	対応する被害	主な設計思想
判断を止めない	認知的ハーム	分散型知識, 継続判断, 制度的記憶の維持
信頼を壊さない	関係的ハーム	公正性, 透明性, 説明責任, 心理的契約維持
人を壊さない	感情的ハーム	心理的安全性, 負荷緩和, 支援と回復

これらの原則は、第2章で示した中核構造と、第3章で整理した三層構造に対応している。すなわち、「判断を止めない」は主としてインフラ層およびビジネスプロセス層における認知的損傷の抑制を、「信頼を壊さない」はビジネスプロセス層から人間・文化層へ波及する関係的損傷の抑制を、「人を壊さない」は人間・文化層における感情的損傷の抑制を目的とする。ここで重要なのは、これらの設計原則が単なる倫理的標語ではなく、サイバーハームの伝播構造に対応する機能的条件として位置づけられる点である。

5.2. 戦略的転換：技術中心から人間中心・総合的アプローチへ

この戦略的転換は、表1の三層構造のうち、第1層の損傷を第2層・第3層へと拡大させないための設計転換として理解されるべきである。

組織的サイバーハームへの対応は、従来の技術中心アプローチから、人間中心かつ総合的な戦略への転換を必要とする。この転換は、単なるツール導入ではなく、人間の役割を「脆弱性」から「防御主体・回復資産」へ再定義することを意味する[11][25][26][33]。

表 4 技術中心アプローチと人間中心・総合的アプローチの比較

観点	技術中心（従来）	人間中心・総合的（転換後）
焦点	境界防御, 検知, 封じ込め	行動, 信頼, 文化, 回復, 統治
人間観	弱点, 誤操作要因	能動的防御主体, 検知資産, 回復資産
運用目標	準拠, 停止最小化	実被害最小化, 継続性確保, 信頼回復
姿勢	反応的	予測的・学習的・適応的
成果の評価	技術指標中心	技術指標＋人的・関係的・文化的指標

このアプローチは、技術が防御の重要な構成要素である一方、その効果を最終的に決定するのは人間の判断、報告、連携、学習であるという前提に立つ[11][25][33]。したがって、技術中心の施策は維持されるべきであるが、それを有効化する土台として人間中心設計が不可欠である。

5.3. ハーム伝播の遮断戦略

サイバーハームは、情報システムから組織機能へ、さらに社会的信頼へと連鎖的に拡大する[1][3]。したがって、本戦略の目的は、ハーム発生後に結果を受け止めることだけではなく、その伝播接点に介入して連鎖を遮断することにある。

第一に、初期発生段階では、従業員を「最弱の環」ではなく「最前線の検知主体」として位置づける必要がある。Bada と Sasse が示すように、単なる啓発中心の施策は行動変容に結びつきにくく、日常業務に根ざした理解可能で実行可能な設計が必要である[33]。ここでは、不審挙動の報告しやすさ、報告後の扱いの公正性、早期通報が評価される仕組みが重要になる。

第二に、内部連鎖の遮断では、報告遅延と責任回避を生まない環境づくりが決定的である。心理的安全性の低い組織では、責任追及が情報共有を抑制し、判断遅延が被害を拡大させる[7][19]。これに対し、公正で非懲罰的な報告環境は、初動の速さと協働の質を高め、被害局所化に資する[30][31][32]。

第三に、外部連鎖の抑制では、迅速かつ誠実な情報共有が不可欠である。情報漏えい後の説明の仕方は、それ自体が市場・顧客・取引先への重要な信号となる[12][13][34]。このため、対外説明は法的リスク対応の一部であるだけでなく、ハームの二次増幅を防ぐ戦略行為として位置づけられるべきである。

5.4. 実装レベルでの具体戦略

本節では、三層構造および三つの設計原則に即して、実装レベルでの具体戦略を示す。すなわち、第1層・第2層では判断停止を回避する設計、第2層・第3層では信頼維持を支える設計、第3層では感情的疲弊を抑制する設計が中心となる。

認知的ハームへの対応としては、分散型知能と訓練が重要である。具体的には、データ不在や通信断を前提とした演習、手動プロセスの再確認、暗黙知の形式知化、役割交代可能性の確保などにより、判断停止の回避と制度的記憶の維持を図る[28][29]。これは単なる手順書整備ではなく、知識が特定個人や特定システムに集中しないよう設計することである。

関係のハームへの対応としては、制度的信頼の再構築が必要である。これには、非難しない報告文化、透明性の高い対内説明、対外的な迅速な情報共有、被害者や関係者への配慮ある対応が含まれる[12][13][15][30][31][32]。組織正義の観点からみれば、結果が不利であっても、手続と説明が公正であると認識されることが、信頼の毀損を抑えるうえで重要である[30][31][32]。

感情的ハームへの対応としては、心理的レジリエンスの確保が必要である。具体的には、インシデント対応チームへの心理的支援、人事部門や管理職の関与、長時間対応後の負荷調整、責任追及よりも構造改善に焦点を当てた振り返りの制度化が求められる[7][14][19][25]。感情的疲弊は個人の弱さではなく、設計不全の結果でもあるという前提が重要である。

5.5. 組織文化としてのレジリエンス構築

レジリエントな組織は、「責任と恥」に基づく文化から、「心理的安全性と共同責任」に基づく文化へ移行する必要がある。この移行を支える要素としては、第一に経営層の明示的関与、第二に非処罰的報告経路の整備、第三に安全行動への肯定的強化、第四に日常業務に埋め込まれた継続教育が挙げられる[11][19][30][31][32][33]。ここでいう文化とは抽象的な価値観ではなく、誰が何を報告でき、どのように扱われ、失敗から何を学ぶかを規定する具体的実践の総体である。

5.6. AI（人工知能）と人間の協働による防御強化

近年において、AI は人間の補助的役割にとどまらず、異常検知、優先順位付け、誤検知の低減、対応負荷軽減に資する実装手段として実用段階に入っている[35][36]。IBM の報告は、AI を広範に活用している組織では、侵害の特定と封じ込めの迅速化や費用削減がみられることを示している[35]。Ponemon の調査も、AI が脅威検知、生産性向上、未知の脅威の発見に有効である一方、運用スキル不足、全社的統制の困難、プライバシー管理の不備が課題であることを示している[36]。

したがって、AI の導入は単なる効率化ではなく、人間の認知負荷を下げつつ、意思決定能力を補強する設計として位置づける必要がある。ただし、NIST の AI リスク管理枠組みが示すように、AI には統治、説明可能性、安全性、透明性、プライバシー、公平性を含む信頼性要件が伴う[37]。よって、AI と人間の協働は、「AI が判断し、人間が追認する」構図ではなく、「AI が補助し、人間が説明責任を負う」構図として設計されなければならない。

5.7. 政策・実践への提言: 概念的実装モデル

以下に示す段階的実装モデルは、本章が提示した三設計原則を組織内に定着させるための、概念的かつ例示的な初期導入モデルである。ここで示す各段階は、文化変革そのものを短期間で完了させることを意味するものではなく、人間中心サイバーレジリエンスへの転換を開始するための初動段階を可視化したものである。各段階の具体的内容および期間は、組織規模、業種、セキュリティ成熟度に応じて調整されるべきであり、本モデルはそのまま適用される標準手順ではなく、実務経験と既存知見を踏まえた仮説的枠組みとして提示する。

表 5 人間中心アプローチ定着に向けた導入初期フェーズ

段階	フォーカス	主な施策
第1段階	基礎構築・経営関与	経営層による方針宣言、非処罰的報告方針の明文化
第2段階	参加促進・行動変容	短時間学習、報告行動の評価、現場での対話
第3段階	実践統合	演習、即時フィードバック、使いやすさ監査
第4段階	定着・改善	指標転換、定例共有、学習ループの制度化

成果指標としては、報告件数、初動検知時間、復旧までの判断時間、従業員の心理的安全性、外部説明の迅速性と一貫性などが考えられる[35][36][37]。重要なのは、失敗件数のみを数えるのではなく、「どれだけ早く気づき、どれだけ誠実に伝え、どれだけ学習へ接続できたか」を評価軸に含めることである。

もっとも、これらの「どれだけ」は一律の単一指標で測定されるものではなく、業種、組織規模、社会的責任の大きさ、業務停止許容度などに応じて設計される必要がある。たとえば、初動検知時間、初回対外説明までの時間、復旧後の業務定着率、被害者対応完了率、信頼回復に関する従業員・顧客調査などは、代表的な候補指標となりうる。今後は、こうした指標群を業種横断的および事例別に比較し、サイバーハームの評価軸としてどこまで汎用化できるかを実証的に検討する必要がある。

6. さいごに

本稿は、組織的サイバーハームを単なる技術的障害としてではなく、認知・関係・感情の三中核領域を起点として組織内外に連鎖的に波及する多次元的現象として再定義することを試みた。Agrafiotis らの分類枠組み[1]、Caplan の危機理論[17][18]、レジリエンス工学[16][25]、制度的裏切り理論[15]、組織正義研究[30][31][32]等の検討に加え、アサヒグループホールディングス事案およびアスクル事案の分析を通じて、技術的防御のみでは現代のサイバー事案の実態に十分対応しきれないことを示した[20][21][22][23]。

サイバーハームは、情報システムの障害から始まり、業務の停止、信頼の揺らぎ、経済的損失、心理的疲弊、社会的影響へと段階的かつ複合的に拡大する。この波及過程を断ち切るためには、人間を「脆弱性」ではなく「最大の防御資産」として位置づける人間中心アプローチへの転換が不可欠である[11][16][19][25][33]。その際に重要なのは、技術的防御を軽視することではなく、それを有効化し、補完し、回復へ接続する組織設計の側面を同時に強化することである。

今後の課題としては、本稿が提示した人間中心の設計原則および実装戦略の有効性を、業種、規模、文化的背景の異なる組織において実証的に検証することが挙げられる。また、AI の活用が進むなかで、検知精度や運用効率の向上と、統治、説明可能性、プライバシー保護をどのように両立させるかも重要な論点である[35][36][37]。政策的観点からは、技術的対策への投資と同等の重みで、人的資本、組織文化、心理的支援、対話的説明責任への投資を制度化していく必要がある。

人間を中核に据えたサイバーレジリエンスは、単なる防御戦略ではない。それは、デジタル時代において組織が壊れず、学び続け、信頼を維持しながら機能し続けるための基盤である。組織的サイバーハームに対する有効な応答は、技術の高度化だけでは完成せず、人間、文化、制度、技術を統合する設計思想のなかで初めて成立するものである。

本稿は論説として理論的統合と事例に基づく探索的検討を行ったものであり、提示した評価指標および実装戦略の有効性については、今後の実証研究による検証が必要である。

参考文献

- [1] Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S. and Upton, D., "A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate," *Journal of Cybersecurity*, Vol.4, No.1, 2018, ty006.
- [2] Lindsey, C. and Glasser, G., "Measuring, qualifying and quantifying the harms of cyber-attacks," CyberPeace Institute, 2024.
- [3] Romanosky, S., "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, Vol.2, No.2, 2016, pp.121-135.
- [4] Ministry of Economy, Trade and Industry, "Cybersecurity Management Guidelines Ver. 3.0," 2023.
- [5] National Center of Incident Readiness and Strategy for Cybersecurity, "Overview of Cybersecurity 2024," 2024.
- [6] Cains, M.G., Flora, L., Taber, D., King, Z. and Henshel, D.S., "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Analysis*, Vol.42, No.8, 2022, pp.1643-1669.
- [7] Islam, E., Rudolph, C. and Oliver, G., "Managing cyber harm: a survey of challenges, practices, and opportunities," *Information Security Journal: A Global Perspective*, Vol.34, No.5, 2025, pp.424-454.
- [8] Stine, K., Quinn, S.D., Witte, G. and Gardner, R., "Integrating Cybersecurity and Enterprise Risk Management (ERM)," NIST Interagency Report 8286, 2020.
- [9] Weick, K.E., "The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster," *Administrative Science Quarterly*, Vol.38, No.4, 1993, pp.628-652.
- [10] Barrot, J.N. and Sauvagnat, J., "Input Specificity and the Propagation of Idiosyncratic Shocks in Production Networks," *Quarterly Journal of Economics*, Vol.131, No.3, 2016, pp.1543-1592.
- [11] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," 2019.
- [12] Gwebu, K.L., Wang, J. and Wang, L., "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems*, Vol.35, No.2, 2018, pp.683-714.
- [13] Kuipers, S.L. and Schonheit, M., "Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises," *Corporate Reputation Review*, Vol.25, No.3, 2022, pp.176-197.
- [14] Litz, B.T., Stein, N., Delaney, E., Lebowitz, L., Nash, W. P., Silva, C. and Maguen, S., "Moral Injury and Moral Repair in War Veterans: A Preliminary Model and Intervention Strategy," *Clinical Psychology Review*, Vol.29, No.8, 2009, pp.695-706.
- [15] Smith, C.P. and Freyd, J.J., "Institutional Betrayal," *American Psychologist*, Vol.69, No.6, 2014, pp.575-587.
- [16] Woods, D. D., "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering," *Reliability Engineering & System Safety*, Vol.141, 2015, pp.5-9.
- [17] Caplan, G., *Principles of Preventive Psychiatry*, Basic Books, New York, 1964.
- [18] Fink, S.L., Beak, J. and Taddeo, K., "Organizational Crisis and Change," *The Journal of Applied Behavioral Science*, Vol.7, No.1, 1971, pp.15-37.
- [19] Cram, W.A., Proudfoot, J.G. and D'Arcy, J., "When Enough is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue," *Information Systems Journal*, Vol.31, No.4, 2021, pp.521-549.
- [20] Asahi Group Holdings, Ltd., "Notice of System Failure Due to Cyberattack," 2025.
- [21] アサヒグループホールディングス株式会社, "サイバー攻撃による情報漏えいに関する調査結果と今後の対応について," 2025.
- [22] アスクル株式会社, "アスクルのサイバーセキュリティ," 2025.
- [23] アスクル株式会社, "ランサムウェア攻撃の影響調査結果および安全性強化に向けた対応策について," 2025.
- [24] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S., "Measuring the Cost of Cybercrime," in Böhme, R. (Ed.), *The Economics of Information Security and Privacy*, Springer, 2013, pp.265-300.
- [25] Hollnagel, E., *Safety-I and Safety-II: The Past and Future of Safety Management*, Ashgate, 2014.
- [26] Dunn Cavelty, M. and Wenger, A. (Eds.), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Routledge, 2022.
- [27] Bouveret, A., "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," IMF Working Paper 18/143, 2018.
- [28] Wegner, D.M., "Transactive Memory: A Contemporary Analysis of the Group Mind," in Mullen, B. and Goethals, G. R. (Eds.), *Theories of Group Behavior*, Springer, 1987, pp.185-208.
- [29] Lewis, K., "Measuring Transactive Memory Systems in the Field: Scale Development and Validation," *Journal of Applied Psychology*, Vol.88, No.4, 2003, pp.587-604.
- [30] Greenberg, J., "Organizational Justice: Yesterday, Today, and Tomorrow," *Journal of Management*, Vol.16, No.2, 1990, pp.399-432.

- [31]Colquitt, J.A., "On the Dimensionality of Organizational Justice: A Construct Validation of a Measure," Journal of Applied Psychology, Vol.86, No.3, 2001, pp.386-400.
- [32]Colquitt, J.A., Conlon, D. E., Wesson, M. J., Porter, C. O. L. H. and Ng, K. Y., "Justice at the Millennium: A Meta-Analytic Review of 25 Years of Organizational Justice Research," Journal of Applied Psychology, Vol.86, No.3, 2001, pp.425-445.
- [33]IBM Security, "Cost of a Data Breach Report 2025," 2025.
- [34]Spence, M., "Job Market Signaling," The Quarterly Journal of Economics, Vol.87, No.3, 1973, pp.355-374.
- [35]Bada, M. and Sasse, A. M., "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?" International Conference on Cyber Security for Sustainable Society, 2015.
- [36]Ponemon Institute, "The 2024 Study on the State of AI in Cybersecurity," 2024.
- [37]National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, 2023.

著者略歴

蓮見 祥子（はすみ・さちこ）

横浜緑ヶ丘高等学校卒業。プリンス・オブ・ソンクラー大学交換留学を経て、ウーロンゴン大学卒業。南クイーンズランド大学にて情報処理学修士・MBAを修了。国際金融機関、OECD、国連機関、国内大手製造業・大手金融機関において25年以上にわたり情報処理、サイバーセキュリティと組織リスク管理に従事。CISOおよび国連CISOグループ共同議長を歴任。2025年より大手コーヒーチェーンサイバーセキュリティ部部長。(ISC)² CISSP, CCSP, ISACA CISA, CRISC, CISM, ICF 認定プロフェッショナル・コーチ、メンタルケア専門心理士。