［論説］

# AI 時代のサイバーセキュリティにおける サイバー判断力の必要性と育成方法 —人的要素強化への実践的提案—

# Cyber Judgment in AI-Era Cybersecurity: A Practical Proposal for Cultivating Human Capabilities

蓮見 祥子†
Sachiko Hasumi

**要旨**

AI 主導型サイバー攻撃の台頭により，人間側の「Cyber Judgment（サイバー判断力）」の欠如が深刻化している．攻撃者は AI により侵入作業を自律化し，攻撃は機械速度へ移行．開封率が非常に高い AI 生成フィッシングなどにより，「機械速度の攻撃者 vs 人間速度の防御者」という非対称性が生まれ，従来の意識啓発研修は限界を迎えている．本論説は失敗の根因を「経験の欠如」と捉え，知覚・解釈・行動の各段階で生じる障壁を指摘．対策として，(1) 体験型学習による経験の獲得，(2) 判断習慣の神経回路レベルでの自動化，(3) 人事制度への統合による組織能力化，の三本柱を提示し，判断速度・精度の向上と国家的レジリエンス強化を展望する．

**Abstract**

This paper proposes a practical, theory-based framework for cultivating Cyber Judgment, an essential yet underdeveloped human capability, by integrating neuroscience, behavioral science, and organizational psychology. The urgency of this framework has escalated with the rise of AI-driven cyberattacks. In 2025, Anthropic reported that state-backed attackers used AI to autonomously execute a substantial portion of intrusion tasks, enabling machine-speed operations and incredibly high open-rate phishing. This creates a structural asymmetrical, machine-speed attackers vs. human-speed defenders that traditional awareness training cannot address. Identifying the root cause of judgment failure as a lack of experiential learning, the paper highlights breakdowns in perception, interpretation, and action. It presents a three-pillar solution: (1) immersive experiential training to build cyber experience, (2) neural-habit formation for automatic micro-judgments, and (3) institutionalization to embed the capability organizationally through integration with human resource frameworks. Anticipated outcomes include faster and more accurate judgments, reduced human-factor incidents, and strengthened national cyber resilience.

## 1. はじめに

私たちは今，サイバー攻撃の本質が根本的に変化する歴史的転換点に立っている．2025 年，アンスロピック（Anthropic）は衝撃的な事実を明らかにした．中国の国家支援型攻撃者が AI（人工知能）システムを用い，侵入作戦の最大 90%を自律的に実行し，世界 30 の標的に対してサイバースパイ活動を展開していたのである[1]．これはシミュレーションではなく，実際に確認された攻撃である．この事例は，サイバー攻撃が「AI 支援による人間主導」から「人間が監督する AI 主導」へと移行しつつあるという新たな現実を示している．

日本は特に脆弱な立場にある．国内企業の 99%以上を中小企業が占め[2]，デジタル人材は慢性的に不足している．どれほど高度なセキュリティツールを導入したとしても，最終的に判断を下すのは人間である．そして今，その人間の判断力こそが，最も弱く，同時に最も重要な防御層となっているのである．

### 1.1. Cyber Judgment（サイバー判断力）：欠落した能力の定義

セキュリティ意識向上トレーニングやフィッシングシミュレーションは，人間の防御能力強化に一定の効果を示し，行動変容も測定可能である．しかし，これらの施策には根本的に欠けている要素がある．それを補う概念が，ガートナー（Gartner）が提唱する「Cyber Judgment（サイバー判断力）」である[3]．ガートナーはサイバー判断力を次のように定義している．「個人が日常業務においてサイバーセキュリティリスクを自律的に評価し，文脈を認識した，リスク情報に基づく意思決定を行う能力」[4]．これは

［論説］
2025 年 11 月 29 日受付, 2025 年 12 月 29 日受理

道路を横断する際の判断に例えることができる．私たちは周囲の交通状況を評価し，リスクを判断し，安全かどうかを瞬時に決定する．無数の繰り返しを通じて，それは自然に行える第二の天性となる．サイバー判断力は，従来の「知識付与」や「行動矯正」を中心とするアプローチとは本質的に異なり，意思決定そのものの質を高める概念である．表 1 に，従来アプローチとサイバー判断力の本質的な違いを整理した．従来型が「何が危険か」を教え，ルール遵守や指示待ちを前提とするのに対し，サイバー判断力は「どう判断し行動するか」に焦点を当て，批判的思考と自律的意思決定を重視する．この対比により，単なる知識の蓄積では不十分であり，文脈に応じた判断能力の育成が不可欠であることが明確になる．

**表 1**　従来アプローチとサイバー判断力比較 [3] [4]

| 従来アプローチ | サイバー判断力 |
|---|---|
| 意識向上（何が危険かを知る） | 判断力育成（どう判断し行動するか） |
| ルール遵守（言われた通りにする） | 批判的思考（なぜそうするのか理解する） |
| トップダウン管理（指示を待つ） | 自律的意思決定（状況に応じて判断する） |

### 1.2. 本論説の目的

本論説の目的は，AI 時代のサイバーセキュリティにおいて真に有効な人的防御層を構築するための，サイバー判断力育成の実践的枠組みを提案することである．具体的には，

1. サイバー判断力が「欠落した能力」である理由を構造的に解明すること
2. 自律的判断力を習慣として定着させる実践的方法論を提示すること
3. 日本企業の文脈に適合した実装戦略を示すこと

## 2. 現状分析：なぜサイバー判断は失敗するのか

### 2.1. AI による攻撃手法（TTP）の根本的変容

AI による攻撃手法は，戦術・技術・手順(TTP)の各要素において根本的な変容を遂げている．まず戦術面では，AI 生成フィッシングの開封率が 72%に達するなど従来の手口を大きく上回る効果を示し[5]，防御システムを回避する行動が自動的に最適化され，重要データ資産を効率的に特定・優先化することが容易になっている．技術面では，数千の標的を短時間で評価する大規模自動偵察，感染のたびに自己変異するポリモーフィック・マルウェア，セキュリティ AI そのものを欺く敵対的機械学習攻撃，さらには経営層の音声や映像を精巧に偽造するディープフェイク詐欺といった新たな攻撃手法が実用段階に入っている[5][6]．さらに手順面では，脆弱性発見から悪用までが数時間以内に行われ，侵入タスクの 80〜90%が自律的に実行され，攻撃経路もリアルタイムに適応し続けるという，機械速度での攻撃プロセスが成立している[1]．その結果，攻撃の規模とスピードは，人間の防御者が対応可能な速度を完全に超過しており，サイバー防御の前提そのものを揺るがす状況となっている．

### 2.2. サイバーキルチェーン全体の圧縮

従来，サイバー攻撃はサイバーキルチェーンと呼ばれる段階的かつ連続的に進行し，偵察，侵入，横展開，情報窃取といったフェーズを順に踏むのが一般的であった[7]．しかし AI の登場により，この一連のプロセスは劇的に加速し，もはや人間が前提としてきた時間軸は成立しなくなっている．

表 2 に，AI がサイバーキルチェーンの各段階に与えた影響を時間軸の変化として整理した．従来，偵察には数週間を要していたが，AI は数分で実行する．武器化は数日から数時間へ，配信は数時間から数秒へと短縮される．さらに，侵入と横展開は「自動」「自律実行」と表記される通り，もはや人間の時間感覚を超えた領域で進行する．この表が示すのは，単なる効率化ではなく，攻撃の時間的性質そのものの質的転換である．AI は高度な偵察を自動化し，脆弱性の特定から悪用までをほぼ機械速度で実行し，攻撃経路をリアルタイムに適応させることで，従来の段階的攻撃モデルを一体化された高速サイクルへと変質させたのである[1][8][9][10][11][12][13].

結果として，「機械速度の攻撃者」と「人間速度の防御者」という圧倒的な非対称性が現代のサイバーセキュリティを定義する決定的要因となっている．この乖離こそが，防御側がいかに高度なツールを保有していても追随できない根本的な理由であり，人的判断の限界が最も露呈する領域である．ゆえに，AI 時代の防御は従来の延長線上には存在せず，人間の介入速度を補完しうる新たな判断能力と運用モデルの再構築が不可欠である[1][8][9][10][11][12][13].

**表 2**　AI のサイバーキルチェーンへの影響[1]

| キルチェーン段階 | 従来 | AI 活用時 |
|---|---|---|
| 偵察 | 数週間 | 数分 |
| 武器化 | 数日 | 数時間 |
| 配信 | 数時間 | 数秒 |
| 侵入 | 数時間 | 自動 |
| 横展開 | 数日 | 自律実行 |

## 2.3. 持続する人間のギャップ

高度な技術的防御システムが導入されても，決定的に弱いまま残されている能力が存在する．それは，人間が適切な判断を，適切なタイミングで，適切な速度で，適切な規模で下す能力である．現状，人間はこの要求に応えられていない[14][15][16]．なぜ従来の意識向上トレーニングは有効に機能しないのか．その理由は明確である．第一に，講義形式の教育では判断力を習得することができないことである[17][18][19][20]．知識の伝達と判断力の育成は本質的に異なるプロセスであり，実際の状況下での経験なしには判断力は発達しない[18][19]．第二に，プレッシャー下において知識を実践へ転用することが困難であるという問題がある．ストレス下では前頭前皮質の機能が低下し[21]，習慣化されていない行動は消失するためである．第三に，人間は機械速度で行動することが不可能である．意識的思考は本質的に遅く，自動化された判断，すなわち習慣がなければ迅速な対応は不可能である[22][23]．第四に，判断そのものが習慣として訓練されていないという構造的欠陥がある．一度きりのトレーニングでは長期記憶に定着せず，反復練習なしには自律的判断力は発達しない[24]．

この人間側のギャップは決定的である．NIST サイバーセキュリティフレームワークの 5 つの機能（識別・防御・検知・対応・復旧）は，いずれも適切なタイミングで人間が判断と意思決定を下すことを前提として設計されている[25]．しかし，機械速度で進行する現代の攻撃環境下においては，人間の認知処理速度の限界により，これらの判断が攻撃の進行速度に追いつかず，フレームワーク全体の実効性は著しく低下している．特に，脅威の検知から対応までの時間的猶予が数分から数秒へと圧縮された状況では，意識的な判断プロセスに依存する従来の人間主導型セキュリティ運用モデルでは，攻撃者に対して決定的な後手を回避できないという構造的脆弱性が顕在化しているのである．どれほど技術的対策が整備されていても，人間の判断が弱ければ最終防御層は破綻し，セキュリティ体制全体を崩壊させる．言い換えれば，人間の判断力の欠如こそが，現代のサイバーセキュリティにおける最大の脆弱性である．

## 2.4. サイバー判断が失敗する 3 つの認知的障壁

効果的な判断は，知覚（Perception），解釈（Interpretation），行動（Action）の 3 つのプロセスから構成される[26]．しかしサイバー環境は，この 3 要素すべてを体系的に阻害する構造を持っている[27]．

**障壁 1：知覚の失敗**

デジタル環境における攻撃兆候は極めて微細である．送信者アドレスの 1 文字の差異，URL(Uniform Resource Locator)のわずかな変異といった特徴は，人間の感覚では容易に見落とされる[28]．人間の感覚記憶は，関連性が低いと判断した情報を自動的にフィルタリングする特性を持つ[29]．巧妙に設計された攻撃シグナル[30]は，このフィルタリングを通過し，知覚段階で検知されないまま残存するのである．

**障壁 2：解釈の失敗**

専門家の直観は，豊富な経験に基づくパターン認識能力によって支えられている．カーネマンとクライン(Kahneman & Klein)は，信頼に足る直観が成立するためには，規則性のある環境と長期的な練習機会が不可欠であると示した[31]．しかし，一般の従業員はサイバー攻撃を直接経験する機会が極めて乏しく[32]，年 1 回程度の訓練では実践的なパターン認識能力を獲得できない．そのため，脅威を意味づけるための経験的メンタルモデルが形成されず，正確な解釈が不可能となるのである．

**障壁 3：行動の失敗**

二重プロセス理論によれば，人間の思考には速いシステム 1 と遅いシステム 2 が存在する[22][23]．未知の状況では人間はシステム 2 に依存するが，これは処理速度が遅く，認知負荷が高く，ストレスの影響を受けやすい．一方，手続き記憶として習慣化されたスキルは高速かつ低負荷で実行でき，ストレス下でも破綻しにくい[33]．しかし，サイバー判断は習慣として訓練されていないため，機械速度で進行す

[1] [1][8][9][10][11][12][13] から抽出したデータを統合して作成した推定値

る攻撃[34]に対して行動が追いつかないという構造的問題が生じているのである．

### 2.5. 根本原因：経験の欠如

サイバー判断が弱いのは，人々が知性を欠いているからではない．原因は，私たちが判断という行為を「経験」として教えてこなかった点にある．認知神経科学と教育学は，効果的な学習には以下の原理が不可欠であることを示している：反復的経験による判断の自動化[35][36]，文脈内での練習による実践場面への転移[37]，間隔反復による長期記憶の形成[38]，感情的関与による記憶定着の強化[39]．

サイバーセキュリティ教育研究は，これらの原理を実証している．ハンズオン型の体験的学習は，従業員のサイバーセキュリティ自己効力感を構築する[40]．リアルなシミュレーション訓練は，実世界への学習転移を促進する[41]．継続的な訓練プログラムは，意識から行動への変化を実現する[42]．

しかし，現実の多くの組織では，これらの原理に反する従来型アプローチが依然として主流である．表 3 に，従来のトレーニング手法が抱える構造的欠陥を整理した．静的なシナリオは理想的状況の理解を提供するが，実践的文脈と認知負荷を欠くため，学習が実務に転移しない．年 1 回のトレーニングは短期記憶に情報を送り込むだけで，長期記憶への定着を実現できず，忘却曲線によって急速に消失する．知識伝達型研修は宣言的知識（何を知っているか）を与えるが，手続き的知識（どう実行するか）を育成しないため，知識と行動の間に深刻なギャップが生じる．この表が示すのは，従来手法の「欠けているもの」こそが，認知神経科学と教育学が不可欠とする学習原理そのものであるという課題である．

したがって，効果的なサイバー判断を構築するためには，知識の伝達に依存する従来型アプローチから，経験的学習を中心に据えるパラダイムシフトが不可欠である．

**表 3** 従来のトレーニングの欠点

| 従来の方法 | 提供するもの | 欠けているもの | 結果 |
|---|---|---|---|
| 静的なシナリオ | 理想的状況の理解 | 実践的文脈と認知負荷 | 転移の失敗 |
| 年 1 回のトレーニング | 短期記憶への情報 | 長期記憶への定着 | 忘却曲線による消失 |
| 知識伝達型研修 | 宣言的知識 | 手続き的知識 | 知識と行動のギャップ |

## 3. 提案内容：自律的サイバー判断力の育成枠組み

### 3.1. 提案の全体像：3 つの柱

本論説は，AI 時代において真に有効な人的防御層を構築するための，自律的サイバー判断力の育成枠組みを提示するものである．その全体像は三つの柱から構成される．第一に，サイバー防災体験型学習施設「サイバーそなエリア」によって，没入型シナリオを通じた経験的学習を実現し，誰もがアクセス可能な形で判断経験を提供することである．第二に，日常業務へ小規模行動を統合し，反復させる習慣形成プログラムによって，自律的判断を自動化することである．第三に，サイバー判断力を組織能力として制度化し，採用・育成・評価へ統合する人事制度上の枠組みを構築することである．

### 3.2. 柱 1：サイバー防災体験型学習施設 サイバーそなエリア

日本は自然災害への備えとして，優れた防災教育インフラを構築してきた．「そなエリア東京」では，地震発生後 72 時間の生存をかけた体験が可能であり，国民に実践的な危機対応能力を身につけさせる仕組みが確立されている．本提案は，この成功モデルをサイバーセキュリティ領域に適用するものである．

#### 3.2.1 サイバーそなエリア（大規模施設版）

「サイバーそなエリア」は，サイバー攻撃の「現場」を体験できる大規模没入型施設である．参加者は，フィッシング攻撃ジオラマ，ランサムウェア感染から復旧までの混乱体験，内部脅威シナリオ，サプライチェーン侵害の追跡，BEC（ビジネスメール詐欺）対応判断，さらにインシデントエスカレーション時のコミュニケーション訓練といった多様なシナリオに直面する．参加者はサイバージオラマ空間を歩きながら実際の攻撃状況下で判断を下し，その選択に対して即時フィードバックを受けることで，判断の適否とその理由を体験的に学習する仕組みである．

従来のセキュリティトレーニングセンターが技術者向け専門内容を中心としてきたのに対し，「サイバーそなエリア」は一般従業員が日常業務で直面する判断そのものに焦点を当てる点に特徴がある．防災教育が特定専門家ではなく市民全体を対象とする基盤教育として確立しているように，サイバー判断も組織に属する全員が備えるべき基礎能力であるという前提に立つ．

### 3.2.2 デジタルサイバー防災車（モバイル版）

デジタルサイバー防災車は，「防災体験車」の発想を応用した移動式サイバー判断訓練車両である．学校，中小企業，地域コミュニティセンターなどを巡回し，ハンズオン型フィッシング・詐欺シミュレーション，VR（仮想現実）/AR（拡張現実）を用いた没入体験，即時フィードバックと個別指導を実施する．これにより，大規模施設にアクセスできない地域や企業に対しても訓練機会を提供できる．

その社会的意義は大きく，地域格差の解消，中小企業支援，高齢者コミュニティの保護，さらには全国民の判断力を底上げする国家デジタルレジリエンス戦略として機能する．また，日本は既に防災体験車を全国に展開し，地域密着型教育を実現してきたという強みを持つ．この既存モデルをサイバー領域に展開することで，世界初の「移動式サイバー判断訓練」を実現できる可能性が高いと言える．

## 3.3. 柱 2：習慣形成プログラム　自律的判断の自動化

体験型学習によって行動として「できる」ようになったとしても，それが日常業務の中で反復的に実践されなければ意味を持たない．サイバー判断の実効性は，神経回路レベルでの習慣化に依存する[33][43]．習慣とは，神経科学的には前頭前皮質から基底核(線条体)への処理の移行として定義される[33][44]．このプロセスは以下の利点をもたらす：

- **認知負荷の劇的な低減**：思考を必要としない自動実行により，判断に必要な精神的リソースを解放する
- **実行速度の向上**：意識的な処理を必要とせず，即座に反応できる
- **ストレス環境下での信頼性**：高負荷状況でも破綻しにくい安定した実行

習慣形成の神経メカニズムは「Cue（きっかけ）-Routine（習慣的行動）-Reward（報酬）」の三段階ループで説明される[45][46]．このループが反復されることで，皮質-基底核回路がチャンキング(行動の塊化)プロセスを通じて強化される[43][46].

表 4 に，この Cue-Routine-Reward ループをサイバー判断の実務場面に適用した具体例を示した．Cue（きっかけ）として「予期しないメールの受信」という日常的な状況を設定し，Routine（習慣的行動）では「リンクを開く前に 5 秒間の検証プロトコル」を実行する．この検証には，送信者ドメイン確認，文面の文法チェック，緊急性の評価といった複数の判断要素が含まれるが，習慣化により一連の行動が自動的に実行される．Reward（報酬）として，安全確認の達成感または脅威回避の安心感が得られることで，このループが神経回路に強化される．この表が示すのは，抽象的な神経科学理論が実務上の具体的行動パターンへと翻訳可能であるということであり，組織がこのフレームワークを用いて従業員の判断習慣を意図的に設計できることを意味する．

**表 4**　サイバー判断における習慣ループの実装例

| フェーズ | 要素 | 実装例 |
|---|---|---|
| Cue（きっかけ） | 特定の状況的トリガー | 予期しないメールの受信 |
| Routine（習慣的行動） | 自動化された判断プロトコル | リンクを開く前に 5 秒間の検証（送信者ドメイン確認，文面の文法チェック，緊急性の評価） |
| Reward（報酬） | 正のフィードバック | 安全確認の達成感，または脅威回避の安心感 |

サイバー判断の有効性は，知識の蓄積ではなく神経回路の習慣化にあり，これにより機械速度の攻撃に対しても即座に反応できる防御能力が確立される[33][44].

### 3.3.1 日常的サイバー判断習慣の構築

理論的基盤を実践に移すためには，以下の小規模な行動を日常業務に統合し，反復することで自動化することが重要となる[43][45].

**1. 「5 秒リンク検査」**

メールやメッセージのリンクをクリックする前に 5 秒間確認し，送信者の正当性，URL のホバー表示，文脈との整合性を確認する行動である．この短時間の検証プロセスが習慣化されることで，視覚的手がかり(Cue)に対する自動的な検証反応(Routine)が形成される[28][33].

**2. 「共有前の一時停止」ルール**

機密情報や個人情報を共有する前に意識的に立ち止まり，受信者の正当性，共有の必要性，適切な方法を確認する．この「一時停止」は，前頭前皮質による意識的な介入から，基底核による自動的な安全確認プロトコルへと移行する[44].

**3.「送信者正当性スキャン」**

予期しない依頼や緊急性を装うリクエストに対して自動的に疑念を抱き，既知の電話番号への折り返しなど代替チャネルで確認する．社会工学的攻撃は「緊急性」という感情的圧力を利用するため[30]，この習慣は感情的反応を冷却する神経的バッファーとして機能する．

**4.「ワンクリック報告反射」**

不審な活動を検知した瞬間に即座に報告し，「後で報告する」という先延ばしを排除する．報告行動が自動化されることで，組織全体の脅威検知速度が機械的攻撃速度に近づく[34].

**5.「マイクロリスク評価プロンプト」**

日常的な意思決定の際に「これはいつもと違うか」「なぜ今このリクエストが来たのか」といった小規模なリスク評価を行う．この自己問診プロセスは，異常検知パターンを神経回路に刻み込むトレーニングとなる[31][33].

これらの行動は，運転時にミラーを確認する動作と同様に，前意識的かつ自動的に実行される必要がある[33][43]. 意識的努力に依存しないレベルまで習慣化されて初めて，サイバー判断力は実践的な防御能力として機能するのである．カーネマンとクライン（Kahneman & Klein）が示したように，信頼に足る直観(expert intuition)は規則性のある環境での長期的練習によってのみ形成される[31]. サイバー判断習慣の構築は，まさにこの「規則性のある練習環境」を意図的に設計し，神経回路レベルでの自動化を達成するプロセスである．

### 3.4. 柱 3：人事制度への統合 組織能力としての制度化

サイバー判断力は単なる IT（情報処理）トレーニングの対象ではなく，組織文化および人材マネジメントと密接に関わる能力である．このため，技術部門のみが担うべき課題ではなく，人事部門が主体となって制度として定着させなければ，文化変革は成功しない．まず採用においては，好奇心を持ち「なぜ」を問う姿勢，異常を検知するパターン認識能力，さらには疑問や失敗を適切に報告できる心理的安全性といった資質を重視する必要がある．選考プロセスには，判断力を測定するシナリオ評価，サイバー判断適性テスト，過去の判断事例に関する質問を組み込み，候補者の基礎的判断能力を多面的に評価することが望ましい．

オンボーディングにおいては，入社初日からサイバーそなエリアを活用した基礎的訓練を実施し，役割別のリスクプロファイルを評価したうえで，初期 90 日間に習慣形成プログラムを組み込むことで，自律的判断力の早期定着を図るべきである．リーダーシップ開発においては，管理職が安全な報告文化を強化し，良い判断を自ら示し，失敗を含めて透明性を確保するモデルとなることが不可欠である．訓練内容には，インシデント対応時のコミュニケーション，心理的安全性の構築，判断ミスに対する建設的フィードバックを含めることで，チーム全体の判断力向上を支援する枠組みが整う．

さらに，パフォーマンス管理では，不審活動の報告頻度と速度，インシデント時の適切な判断，セキュリティとビジネス要件の調和といった行動指標を評価項目として統合する必要がある．具体的には，「疑わしい事象を一定回数報告した」「インシデント発生時に所定時間内でエスカレーションした」「ビジネス要件とセキュリティ要件の適切な調整を行った」など，行動として観察可能な基準を用いることで，判断行動を制度的に評価可能な形へと位置づけることができる．

文化設計においては，早期報告に対する報酬や称賛，良い判断の可視化と共有，セキュリティチャンピオン制度の導入などを通じて，望ましい判断行動を文化的規範として強化することが求められる．同時に，「失敗は学習の機会である」という明確な原則を組織として提示し，心理的安全性を確保することが不可欠である．フィッシング訓練では罰ではなく教育を重視し，判断ミスを個人の責任追及の材料とするのではなく，システム改善に向けた出発点として扱う姿勢が必要である．

以上のように，人事制度全体にサイバー判断力を統合することにより，判断力は個人の属人的能力ではなく，組織の持続的能力として制度化される．これにより，組織は長期的な競争力とレジリエンスを確保する基盤を構築することが可能となるのである．

## 4. 理論的根拠：なぜこの提案が有効なのか

### 4.1 経験的学習の神経科学的基盤

人間の記憶は三つのシステムから構成されている[47]. 第一にエピソード記憶であり，これは「いつ，

どこで，何が起こったか」という個人的経験の記憶である．サイバーそなエリアでの体験は強力なエピソード記憶を形成し，実際の攻撃に直面した際に「あの時の体験」が想起される契機となる．第二に意味記憶であり，事実や概念に関する記憶である．従来の研修は主としてこの領域を対象としてきたが，これだけでは行動変容には不十分である．第三に手続き記憶であり，スキルや習慣に関する記憶である．習慣形成プログラムはこの記憶を構築し，意識的努力を必要としない実行を可能にする．

効果的なサイバー判断力育成には，この三つを統合することが不可欠である．サイバーそなエリアはエピソード記憶と意味記憶を構築し，習慣形成プログラムは手続き記憶を構築し，人事制度への統合はこれらを組織文化として定着させる役割を果たす．エビングハウス忘却曲線研究は，情報の大部分が学習後 24 時間以内に失われることを示している[24]が，間隔をあけた反復は長期記憶への定着を劇的に改善することも明らかである[38]．この観点から，サイバーそなエリアへの初回訪問，3 か月後，6 か月後，そして年次訪問というスケジュール設計は合理的であり，デジタルサイバー防災車による 3〜6 か月ごとの巡回は地域単位での間隔反復を実現する仕組みとなる．

### 4.2 習慣形成の行動科学的根拠

行動科学の研究は，小規模で具体的な行動の反復が，大規模で抽象的な目標より効果的であることを示している[48]．実装意図（implementation intention）理論によれば，「いつ・どこで・どのように行動するか」を明確に定めた具体的な計画は，抽象的な目標設定に比べて目標達成率を大幅に向上させる[48]．「セキュリティ意識を高める」といった抽象的目標は測定不能であり，具体的行動に結びつかない．その一方，「メールのリンクをクリックする前に 5 秒待つ」といった具体的行動は測定可能であり，即座に実行可能であり，反復により自動化される．

さらに，状況的認知理論は，実験室的学習は実際の文脈への転移が困難であり，学習と実践が同一文脈で行われることが効果的転移の鍵となることを示している[49]．Brown， Collins & Duguid (1989) は，知識は使用される文脈と切り離せないものであり，真正な活動の中でこそ効果的に習得されると論じている[49]．サイバーそなエリアは実際の業務環境を模倣し，時間的プレッシャーや不確実性を再現し，実際に使用するツールを用いる点で優れている．また習慣形成プログラムは日常業務に直接統合され，反復と即時フィードバックを可能とする．

### 4.3 組織文化変革の社会心理学的基盤

組織文化研究は，文化は規則や方針では変わらず，反復された経験によって変化することを示している[50]．Schein (1996)は，組織文化を「集団が外部適応と内部統合の問題を解決する過程で学習した，共有された基本的仮定のパターン」と定義し，文化は観察可能な行動の反復と，それが成功をもたらすという学習経験を通じて形成されると論じている[50].「ポリシーを読んで署名する」「年 1 回の義務研修」「トップダウンの命令」といった手法は文化を変えない．機能するのは，日々の小さな成功体験の積み重ね，リーダーによるモデル化，そして同僚からの承認と支援である．

したがって文化変革には人事制度への統合が不可欠である．採用は価値観を形作り，評価は何が重要かを示し，報酬は行動を強化し，リーダーシップは規範を設定する．これらはいずれも人事の領域であり，サイバー判断力を人事能力として制度化することで，初めて組織の文化的遺伝子として固定されるのである．

### 4.4 日本の防災文化との親和性

日本が世界トップレベルの災害レジリエンスを持つ理由は，技術だけでなく文化にある．学校や職場での定期訓練，地域コミュニティの関与，経験の共有と継承，そなエリア東京に代表される体験教育インフラなどがその基盤である．

この成功モデルはサイバーセキュリティにも適用可能である．表 5 に，防災における主要な仕組みとサイバーセキュリティへの対応関係を整理した．防災訓練における「避難訓練」は，サイバー領域では「サイバー判断演習」として実装できる．移動式の「防災体験車」は，組織や学校を巡回する「デジタルサイバー防災車」に対応し，体験型学習を広く提供する．「地域防災組織」のような自律的な相互支援体制は，組織内で判断力を持つ従業員が他者を支援する「組織内セキュリティチャンピオン」として機能する．そして，実物大の災害体験施設である「そなエリア東京」は，没入型のサイバー攻撃シミュレーション環境を提供する「サイバーそなエリア」へと展開可能である．この対応関係が示すのは，日本が既に持つ社会的学習基盤を，新たなインフラ構築なしに概念的に拡張できるということである．

日本は既に生命を守る判断を全国民に教える方法を知っている．今こそ，その知恵をサイバー空間に

適用すべき時である．

**表 5** サイバーセキュリティ防災

| 防災 | サイバーセキュリティ |
|---|---|
| 避難訓練 | サイバー判断演習 |
| 防災体験車 | デジタルサイバー防災車 |
| 地域防災組織 | 組織内セキュリティチャンピオン |
| そなエリア東京 | サイバーそなエリア |

## 5. 想定される効果・影響

### 5.1 期待される成果

本提案を実装することにより，以下の成果が期待できる．ただし，これらは理論的枠組みおよび関連研究に基づく研究目標であり，その達成可能性と実効性については今後の実証実験による検証が必要である．

まず，個人レベルでは判断速度と判断精度の向上を目指す．Wash[28]が示す熟練者の三段階判断プロセス(sense-making，suspicion，confirmation)に基づく訓練により，脅威検知から対応までの時間的遅延の縮小を図る．また，判断精度の向上により誤検知が減少し，真の脅威の検知率が上昇することを目標とする．KnowBe4 の 2025 年業界ベンチマーク調査[51]によれば，体系的な訓練プログラムにより，フィッシングメールへの脆弱性(Phish-prone Percentage)を初期値 34.3%から 12 ヶ月後には 4.6%まで低減できることが示されており，本提案も同等以上の効果を目指す．さらに，Arnsten[21]が示すストレス下での前頭前皮質機能の低下メカニズムを考慮した訓練により，プレッシャー下でも判断能力を維持できるストレス耐性の向上を図り，インシデント対応時のパニック反応の減少を目標とする．

組織レベルでは，ヒューマンエラーを起因とするインシデントの大幅な減少を目指す．Mimecast[16]の 2025 年調査では，人的要因が関与するインシデントが全体の 95%を占めることが報告されており，効果的な訓練プログラムの実装により，この割合の顕著な低減を目標とする．また，インシデントの早期検知と報告速度の向上を図る．IBM Cost of Data Breach Report 2024 [52]によれば，データ侵害の特定に平均 194 日を要することが報告されているが，本提案による判断力の向上と組織文化の醸成により，この期間の大幅な短縮を目指す．特に，発見から内部報告までの時間を短縮することで，被害の最小化を実現する．インシデント管理の効率も改善し，Reeves et al.[32]が指摘するサイバー疲労の軽減により，誤報告の減少と質の高い報告による対応の迅速化を図る．また，セキュリティが「負担」ではなく「能力」として認識されることで従業員のバーンアウトが減少し，組織全体における心理的安全性も向上する．

社会レベルにおいては，国家サイバーレジリエンスの強化を目標とする．全国民のサイバー判断力が底上げされることで，デジタル社会における基盤的能力が構築されるのみならず，中小企業や脆弱なコミュニティの保護にも資する．中小企業庁[2]が指摘する中小企業のサイバーセキュリティ脆弱性に対し，本提案は実践的な対応策を提供する．地域格差の解消や高齢者のデジタル詐欺被害の減少も期待される．さらに，本提案は NIST サイバーセキュリティフレームワーク[25]における識別・防御・検知・対応・復旧の全機能に対し，人的能力の強化という形で横断的に寄与し，フレームワークの実効性を補完・向上させる基盤として機能することを目指す．

なお，AI 時代のサイバーセキュリティ対策としては，本研究で提案する人間のサイバー判断力向上策に加えて，AI 主導の攻撃に対応する AI 主導の防御システムの開発・導入も不可欠である．自動脅威検知，リアルタイム異常検知，自動対応システムなどの AI 防御技術は，Anthropic[1]や NCSC[9][10]が指摘するように，攻撃の高速化・自動化に対抗する上で重要な役割を果たす．しかしながら，AI システムによる自動防御には限界があり，特に未知の脅威や複雑な状況判断が必要な場面では，最終的な意思決定に人間の関与が不可欠である[14]．したがって，本研究で提案する人間の判断力向上策は，AI 防御システムと相補的に機能し，人間と AI の協働による多層防御体制の構築に寄与するものと位置づけられる．この人間と AI の最適な協働関係の構築も，本研究の重要な探究課題である．

### 5.2 適用可能な場面

本提案は多様な領域に適用可能である．まず企業組織においては，全従業員がフィッシングや BEC（ビジネスメール詐欺）といった一般的な脅威に対する判断力を強化し，情報共有時の適切な判断や不審活動の報告能力を向上させることができる．役割別にみれば，経営層には戦略的判断およびインシデント

対応判断が求められ，財務部門には BEC や請求書詐欺への判断力が必要である．人事部門には個人情報保護に関する的確な判断が要求され，営業部門には顧客情報管理に関わる判断が必須となる．

教育機関においては, 学生にとってサイバー判断はデジタルリテラシーの基礎能力として機能し, SNS 上の脅威への対処能力向上にも寄与する．教職員は，学生情報や研究データの保護に関わる判断能力を強化することで，教育現場全体の情報セキュリティ水準を高めることができる．

地域コミュニティにおいても，本提案は有効である．高齢者はデジタル詐欺に対する防御力を高め，オンラインサービス利用時の判断を改善することが可能となる．地方自治体は，住民向けサービスのセキュリティ向上に寄与するとともに，地域のデジタル化を支援する際の基盤として活用できる．

このように，本提案は企業，教育機関，地域社会といった多層的な場面において適用可能であり，日本社会全体のサイバー判断力を底上げする包括的枠組みとして機能するものである．

### 5.3 限界と注意点

本提案には，いくつかの限界と注意点が存在する．第一に，技術的限界である．本提案は人的能力の強化を中心とするものであり，技術的防御を代替するものではない．ファイアウォール，侵入検知システム，アクセス制御といった技術的対策は依然として不可欠であり，サイバー判断力はそれらを補完する「最後の砦」であり，同時に「第一線」として機能するにすぎない．

第二に，実装過程における課題である．サイバーそなエリア施設の建設やデジタルサイバー防災車の開発・運用には相応のコストが発生し，継続的なシナリオ更新やメンテナンスも必要となる．文化変革は一朝一夕に達成できるものではなく，数年単位の継続的取り組みが求められる．加えて，「また新しいトレーニングか」という受容疲れや，人事制度変更に対する組織的抵抗が生じる可能性も否定できない．

第三に, サイバー判断力の測定の困難性が挙げられる．サイバー判断力は本質的に無形の能力であり，「防いだ攻撃」は可視化されないため，改善が長期的かつ漸進的にしか把握できない．他要因との切り分けも容易ではない．この問題に対しては，報告速度や検知率などの代理指標の活用，長期的トレンドの分析，定性的評価との組み合わせといった多角的アプローチが必要である．

第四に，継続的進化の必要性がある．脅威環境は絶えず変化し続けるため，シナリオの定期更新，新たな攻撃手法への適応，さらには AI 技術の進展を踏まえた訓練内容の刷新が不可欠である．サイバー判断力の育成は，一度確立すれば完了する静的な枠組みではなく，継続的に進化させるべき動的プロセスであることを強調しておきたい．

最後に，本研究では人間のサイバー判断力向上に焦点を当てたが，AI 時代のサイバーセキュリティ対策としては, AI 主導の攻撃に対応する AI 主導の防御システム（自動脅威検知，リアルタイム異常検知，自動対応システムなど）の開発・導入も不可欠である．ただし，AI システムによる自動防御には限界があり，特に未知の脅威や複雑な状況判断が必要な場面では，最終的な意思決定に人間の関与が不可欠である．したがって，本研究で提案する人間の判断力向上策は，AI 防御システムと相補的に機能し，人間と AI の協働による多層防御体制の構築に寄与するものと位置づけられる．

## 6. おわりに

### 6.1 主張のまとめ

AI 時代のサイバー攻撃は，人間の意思決定速度を完全に凌駕している．唯一の実行可能な防御は，機械が複製できない能力である人間の判断力を強化することである．本論説は，サイバー判断力が現代サイバーセキュリティにおいて「欠落した能力」となっている理由を，以下の三つの構造的要因から論証した．第一に，従来の防御モデルの前提が崩壊したことである．AI 駆動型攻撃は既知のルールベースの運用では対応不能であり，防御体系そのものの性質を問い直している．第二に，攻撃の速度と規模の非対称性である．専門家の判断を待つ余裕がなく，秒単位の意思決定が必要となる環境下では，従来の人間中心モデルは成立し得ない．第三に，知識の向上と判断の本質的相違である．知識の付与だけでは行動変容は保証されず，判断は学習と経験の積層により形成される独立した能力である．

さらに本論説では，サイバー判断力育成のための三つの柱を提示した．第一の柱である体験型学習施設「サイバーそなエリア」は，大規模没入型施設とモバイル版による民主的アクセスを通じ，日本が強みとしてきた防災教育モデルをサイバー領域に応用する試みである．第二の柱である習慣形成プログラムは，日常業務に統合された小規模行動の反復により，神経科学的に裏付けられた判断の自動化プロセスを促進する枠組みである．第三の柱である人事制度への統合は，サイバー判断力を組織能力として制度化し，文化変革の基盤を構築するものである．これらの枠組みは，認知神経科学，行動科学，組織心

理学の知見に基づき，さらに日本の防災文化という強固な土台を活用することで，実践的かつ持続可能な形で構築可能である．

## 6.2 独自の貢献

本論説の独自性は，以下の四点に集約される．第一に，ガートナーの概念，判断理論，認知神経科学の知見を統合し，理論から実践への具体的橋渡しを行った点である．第二に，防災教育に代表される日本固有の文化的強みを活用し，国内に適合した実装戦略を示した点である．第三に，IT 部門のみならず人事部門の役割を明確化し，文化変革のメカニズムを制度面から解明した点である．第四に，モバイル版による地域格差の解消や，中小企業・高齢者コミュニティへの配慮を通じて，社会的包摂性を重視した点である．

## 6.3 今後の展望

**短期的展望（1〜3 年）**

パイロットプログラムの実施により，先進企業におけるサイバーそなエリア体験，デジタルサイバー防災車の試験運用，習慣形成プログラムの効果測定を進める．また，国家サイバー戦略・教育カリキュラム・中小企業支援策への統合を政策提言として実施する．

**中期的展望（3〜5 年）**

主要都市への施設建設，デジタルサイバー防災車の全国展開，企業・教育機関での標準プログラム化を推進する．また，日本モデルを国際的に展開し，グローバル・ベストプラクティスとして確立する．

**長期的展望（5〜10 年）**

「Everyday Cyber Judgment」を社会に定着させ，世代を超えた判断習慣の継承を進める．同時に，AI 技術の進展に応じて内容更新を行い，新たな脅威に適応する．最終的には，自然災害に備える防災文化に匹敵するサイバーレジリエンス文化を確立し，国際的なベンチマークとしての地位を確立する．

## 6.4 さいごに

日本はすでに，防災教育を通じて「生命を守る判断」を全国民に教える方法を確立している．地震・津波・台風への備えは，日本社会の文化的遺伝子として深く浸透している．同様に，サイバー空間にもこの知恵を応用すべき時期が来ている．セキュリティは文化であり，文化は規則では変わらない．文化を変えるのは，反復された経験である．サイバー判断も同様である．技術のみでは私たちを守れない時代において，人間の判断力を体系的かつ構造的に強化することこそが，持続可能なサイバーセキュリティを実現する唯一の道である．

## 参考文献


[1] Anthropic, "Disrupting the first reported AI-orchestrated cyber espionage campaign," Anthropic Research Reports, 2025, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf, 2025.11.17 参照.

[2] 中小企業庁, "中小企業白書," 経済産業省, 2024, https://www.chusho.meti.go.jp/pamflet/hakusyo/2024/PDF/chusho.html, 2025.11.27 参照.

[3] Gartner, "Human Factors in Cybersecurity," https://www.gartner.com/en/conferences/apac/security-risk-management-australia/featured-topics/human-factors-in-cybersecurity, 2025.11.27 参照.

[4] Gartner, "Drive Secure Employee Behaviors," https://www.gartner.com/en/cybersecurity/insights/drive-secure-employee-behaviors, 2025.11.17 参照.

[5] Ramirez, S., "AI Cyber Attacks Statistics: How Attacks, Deepfakes & Ransomware Have Escalated," SQ Magazine, 2025, https://sqmagazine.co.uk/ai-cyber-attacks-statistics/, 2025.12.04 参照.

[6] Sift, "Index Reports: AI Fraud Q2 2025," 2025, https://sift.com/index-reports-ai-fraud-q2-2025/, 2025.11.27 参照.

[7] Lockheed Martin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, 2011.

[8] Khalil, M., "AI Cybersecurity Threats 2025: How to Survive the AI Arms Race," DeepStrike, 2025, https://deepstrike.io/blog/ai-cybersecurity-threats-2025, 2025.11.17 参照.

[9] NCSC (National Cyber Security Center), "The Near-Term Impact of AI on Cyber Threat," National Cyber Security Centre, https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat, 2025.11.27 参照.

[10] NCSC, "The Impact of AI on Cyber Threat from Now to 2027," National Cyber Security Centre, https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027, 2025.11.17 参照.
[11] Stanham, L., "AI-Powered Cyberattacks," CrowdStrike, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/, 2025.11.27 参照.
[12] AI CERTs, "AI Cybersecurity Threats: Zero-Day Vulnerabilities Hacked Fast," 2025, https://www.aicerts.ai/news/ai-cybersecurity-threats-zero-day-vulnerabilities-hacked-fast/, 2025.11.18 参照.
[13] Sexton, M., "AI and the Evolution of Asymmetric Cyber Warfare: Insights from the 2025 Israel-Iran Conflict," Trends Research, 2025, https://trendsresearch.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/, 2025.11.17 参照.
[14] Goldfarb, A. and Lindsay, J.R., "Prediction and judgment: Why artificial intelligence increases the importance of humans in war," International Security, Vol.46, No.3, 2022, pp.7-50.
[15] Angelo de, D., "Ransomware Speed Crisis," Palo Alto Networks, 2025, https://www.paloaltonetworks.com/blog/2025/09/ransomware-speed-crisis/, 2025.11.27 参照.
[16] Mimecast, "State of Human Risk 2025," 2025, https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/, 2025.11.19 参照.
[17] Prümmer, J., van Steen, T. and van den Berg, B., "A systematic review of current cybersecurity training methods," Computers & Security, Vol.136, 2024, 103585.
[18] Benner, P., "Using the Dreyfus Model of Skill Acquisition to describe and interpret skill acquisition and clinical judgment in nursing practice and education," Bulletin of Science, Technology & Society, Vol.24, No.3, 2004, pp.188-199.
[19] Wilson, B.G. and Myers, K.M., "Situated cognition in theoretical and practical context," Theoretical foundations of learning environments, 2000, pp.57-88.
[20] Rousse, B.S. and Dreyfus, S.E., "Revisiting the six stages of skill acquisition," Teaching and learning for adult skill acquisition: Applying the Dreyfus & Dreyfus model in different fields, 2021, pp.3-27.
[21] Arnsten, A.F., "Stress signalling pathways that impair prefrontal cortex structure and function," Nature Reviews Neuroscience, Vol.10, No.6, 2009, pp.410-422.
[22] Kahneman, D., "Thinking, Fast and Slow," Farrar, Straus and Giroux, 2011.
[23] Evans, J.S.B.T. and Stanovich, K.E., "Dual-process theories of higher cognition: Advancing the debate," Perspectives on Psychological Science, Vol.8, No.3, 2013, pp.223-241.
[24] Ebbinghaus, H., "Über das Gedächtnis," Duncker & Humblot, 1885.
[25] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology (NIST), 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, 2025.11.27 参照.
[26] Santagata, R. and Yeh, C., "The role of perception, interpretation, and decision making in the development of beginning teachers' competence," ZDM Mathematics Education, Vol.48, No.1, 2016, pp.153-165.
[27] Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Listen, D. and Campagna, G., "Leveraging human factors in cybersecurity: An integrated methodological approach," Cognition, Technology & Work, Vol.24, No.2, 2022, pp.365-390.
[28] Wash, R., "How experts detect phishing scam emails," Proceedings of the ACM on Human-Computer Interaction, Vol.4, No.CSCW2, 2020, Article 165.
[29] Cowan, N., "Evolving conceptions of memory storage, selective attention, and their mutual constraints within the human information-processing system," Psychological Bulletin, Vol.104, No.2, 1988, pp.163-191.
[30] Krombholz, K., Hobel, H., Huber, M. and Weippl, E., "Advanced social engineering attacks," Journal of Information Security and Applications, Vol.22, 2015, pp.113-122.
[31] Kahneman, D. and Klein, G., "Conditions for intuitive expertise: A failure to disagree," American Psychologist, Vol.64, No.6, 2009, pp.515-526.
[32] Reeves, A., Delfabbro, P. and Calic, D., "Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue," SAGE Open, Vol.11, No.1, 2021.
[33] Ashby, F.G., Turner, B.O. and Horvitz, J.C., "Cortical and basal ganglia contributions to habit learning and automaticity," Trends in Cognitive Sciences, Vol.14, No.5, 2010, pp.208-215.
[34] Nespoli, P., Papamartzivanos, D., Mármol, F.G. and Kambourakis, G., "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," IEEE Communications Surveys & Tutorials, Vol.20, No.2, 2018, pp.1361-1396.
[35] Anderson, J.R. and Schunn, C.D., "Implications of the ACT-R learning theory: No magic bullets," In Glaser, R. (Ed.), Advances in Instructional Psychology, Vol.5, Routledge, 2013, pp.1-33.
[36] Anderson, J.R., "ACT: A simple theory of complex cognition," American Psychologist, Vol.51, No.4, 1996, pp.355-365.

[37] Anderson, J.R., Reder, L.M. and Simon, H.A., "Situated learning and education," Educational Researcher, Vol.25, No.4, 1996, pp.5-11.
[38] Kang, S.H.K., "Spaced repetition promotes efficient and effective learning: Policy implications for instruction," Policy Insights from the Behavioral and Brain Sciences, Vol.3, No.1, 2016, pp.12-19.
[39] McGaugh, J.L., "The amygdala modulates the consolidation of memories of emotionally arousing experiences," Annual Review of Neuroscience, Vol.27, 2004, pp.1-28.
[40] Konak, A., "Experiential learning builds cybersecurity self-efficacy in K-12 students," Journal of Cybersecurity Education, Research and Practice, Vol.2018, No.1, 2018, Article 6.
[41] Yigit, Y., Kioskli, K., Bishop, L., Chouliaras, N., Platis, D. and Leandros, T., "Enhancing cybersecurity training efficacy: A comprehensive analysis of gamified learning, behavioral strategies and digital twins," In 2024 IEEE 25th international symposium on a world of wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, 2024, pp.24-32.
[42] Ussher-Eke, D., "From awareness to action: Designing effective cybersecurity training programs," International Journal of Science and Research Archive, Vol.16, 2023, pp.494-504.
[43] Graybiel, A.M., "Habits, rituals, and the evaluative brain," Annual Review of Neuroscience, Vol.31, 2008, pp.359-387.
[44] Graybiel, A.M. and Grafton, S.T., "The striatum: Where skills and habits meet," Cold Spring Harbor Perspectives in Biology, Vol.7, No.8, 2015, a021691.
[45] Duhigg, C., "The Power of Habit: Why We Do What We Do in Life and Business," Random House, 2012.
[46] Smith, K.S. and Graybiel, A.M., "Habit formation," Dialogues in Clinical Neuroscience, Vol.18, No.1, 2016, pp.33-43.
[47] Squire, L.R., "Memory systems of the brain: A brief history and current perspective," Neurobiology of Learning and Memory, Vol.82, No.3, 2004, pp.171-177.
[48] Gollwitzer, P.M. and Sheeran, P., "Implementation intentions and goal achievement: A meta-analysis of effects and processes," Advances in Experimental Social Psychology, Vol.38, 2006, pp.69-119.
[49] Brown, J.S., Collins, A. and Duguid, P., "Situated cognition and the culture of learning," Educational Researcher, Vol.18, No.1, 1989, pp.32-42.
[50] Schein, E.H., "Culture: The missing concept in organization studies," Administrative Science Quarterly, Vol.41, No.2, 1996, pp.229-240.
[51] KnowBe4, "2025 Phishing By Industry Benchmarking Report," KnowBe4 Research, 2025, https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report, 2025.11.27 参照.
[52] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Corporation, 2024, https://www.ibm.com/reports/data-breach, 2025.11.27 参照.

## 著者略歴

**蓮見 祥子（はすみ さちこ）**

1994 年横浜緑ヶ丘高等学校卒業．タイ国立プリンス・オブ・ソンクラー大学交換留学．1998 年オーストラリア国立ウーロンゴン大学文学士号政治専攻課程卒業．2003 年オーストラリア国立南クイーンズランド大学情報処理学修士課程修了．2022 年同大学経営学修士課程修了．1998 年～2024 年ステートストリート信託銀行（東京，パリ，ロンドン），OECD（パリ），スタンダードライフ（モントリオール，現マニュライフ），国際連合機関（UNIDO，ICAO，UN Women，IOM）で CISO 及び国連 CISO グループ共同議長，サントリーホールディングス，野村証券勤務，2025 年スターバックスコーヒージャパンサイバーセキュリティ部部長，現在に至る．第一種情報処理技術者，(ISC)² CISSP，CCSP，ISACA CISA，CRISC，CISM，ICF PCC，メンタルケア専門心理士．