なぜ「セキュリティ投資」を増やしてもサイバー攻撃の被害は減らないのか

～「高度化」ではなく「産業化」する脅威への経済的対抗策～

ライフデザイン研究部 主席研究員/テクノロジーリサーチャー 柏村 祐

1.投資と成果の「乖離」

企業のサイバーセキュリティ投資は、過去最大規模に膨れ上がっている。しかし、皮肉なことにサイバー攻撃による被害件数もまた、増大を続けている。例えば、近年発生した国内有数の飲料メーカーや大手オフィス用品通販企業へのランサムウェア攻撃は記憶に新しい。前者は飲食店の供給網に、後者は医療現場の物流に深刻な影響を及ぼし、完全復旧までに数ヶ月単位の時間を要することとなった。これほどの大企業が対策を講じていてもなお、なぜ我々の防御は突破され続けるのか。

多くの企業は、この原因を「攻撃技術の高度化（Sophistication）」にあると捉える傾向にある。メディアが報じる国家支援型ハッカーの脅威を重視し、高額な最新ソリューションの導入こそが解決策であると考える向きも強い。もちろん高度な防御は必要だが、それだけで万全とは言えないのが実情だ。

実際にセキュリティベンダー各社が公表している侵害調査レポート等を見ると、現実は異なる側面を示している。多くの侵害事例において、攻撃手法そのものは既知の脆弱性や安価なツールの組み合わせであり、脅威の本質は技術的な「高度化」よりも、圧倒的な「低コスト化」と「産業化」にあることが浮き彫りになっている。攻撃側はすでに、極めて効率的な分業体制とサプライチェーンを構築し、ROI（投資対効果）を最大化する「ビジネス」として攻撃を実行しているのだ。

本稿では、サイバー空間で起きている構造変化を、攻撃者のインセンティブ構造や費用対効果に着目する「ミクロ経済学」の視点から解き明かす。技術論だけでは見えてこない「攻撃者の経済合理性」を理解した上で、企業が検討すべき戦略転換について提言したい。

2.攻撃コストを劇的に引き下げる「3 つの構造変化」

かつてサイバー攻撃は、一部の天才的な技術者による「職人芸」であった。しかし現在、アダム・スミスが説いた「分業」による生産性向上がサイバー犯罪の世界でも起きており、その参入障壁は完全に崩壊し、誰でも参入可能な「巨大産業」へと変貌を遂げている。その背景には、以下の 3 つの不可逆的な構造変化が存在する。

(1)「RaaS」による攻撃能力の民主化と参入障壁の消滅

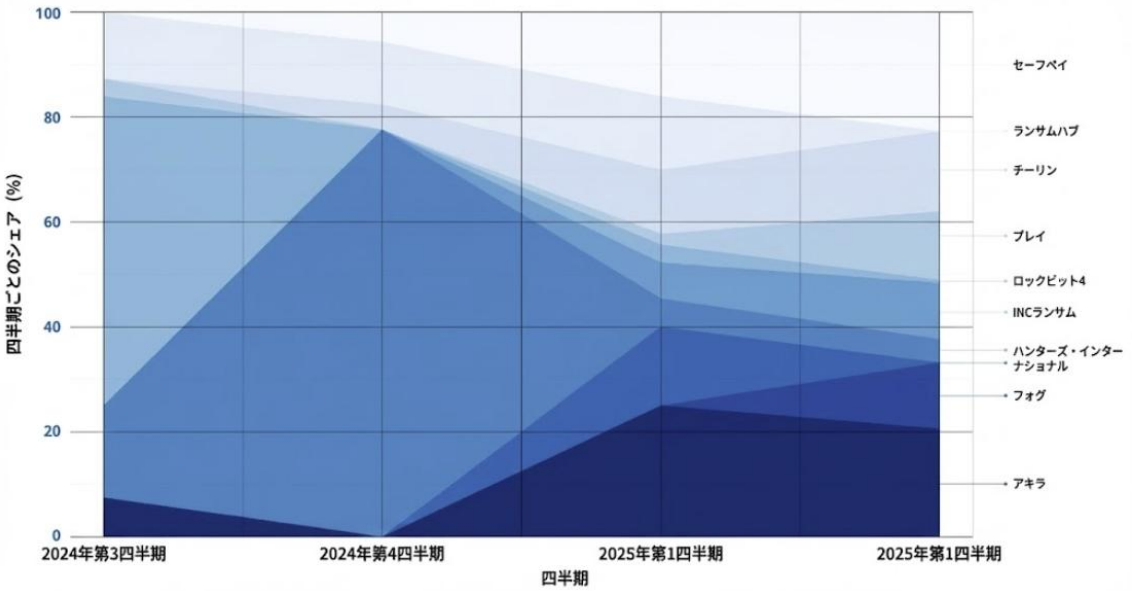
第一にして最大の要因は、攻撃能力そのものが「商品」として流通する「RaaS（Ransomware-as-a-Service）」モデルの定着である。かつて攻撃を実行するには、脆弱性を発見し、エクスプロイトコード（攻撃プログラム）を自作する高度なエンジニアリング能力が不可欠であった。これが自然な参入障壁となり、攻撃者の数を限定的なものに留めていた。

しかし現在は、闇市場において月額サブスクリプションや成果報酬(身代金の分配)を支払うだけで、軍事レベルの攻撃インフラを利用できる。開発者はツールのアップデートに専念し、実行者（アフィリエイト）は攻撃の実務に専念するという、フランチャイズビジネスのような分業体制が完成しているのだ。

ENISA（欧州ネットワーク情報セキュリティ庁）の 2025 年版レポート（注 1）によれば、警察当局が「ロックビット」のような最大手犯罪グループを摘発・解体しても、攻撃の総量は微動だにしていない（図表 1）。ロックビットといえば、名古屋港のコンテナターミナルをシステム障害に追い込み、日本の物流を一時麻痺させた事件などで知られる世界最大級のランサムウェアグループである。しかし、彼らが摘発されても、攻撃者は特定の組織に忠誠を誓っているわけではなく、即座に「アキラ」や「ランサムハブ」といった代替プラットフォームへ乗り換え、事業を継続している。

このデータは、攻撃者がもはや特定の技術に依存しない「単なるサービス利用者」と化していることを如実に示している。技術を持たない素人が、クレジットカード一枚で凶悪なサイバー犯罪者になれる。この「攻撃能力の民主化」こそが、脅威が減らない根本原因である。

図表 1　EU における主要ランサムウェア派生グループのシェア推移（2024 年 Q3～2025 年 Q1）



資料：ENISA Threat Landscape 2025 より筆者作成
*1：大手グループが摘発されても、多種多様な攻撃ツール（RaaS）が代わりに使用され続けていることを示すグラフ。

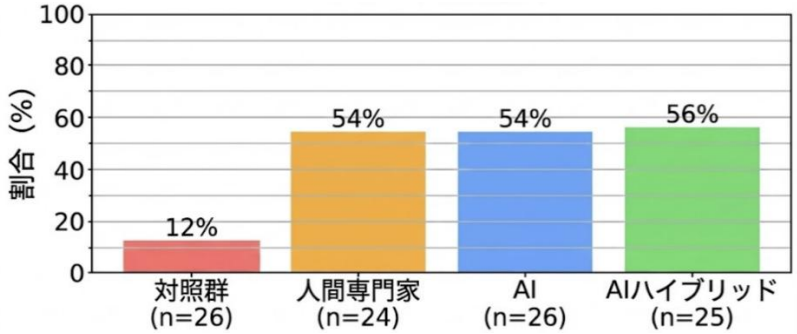
(2)生成 AI による「言語の壁」の崩壊

第二の要因は、生成 AI の悪用による「騙し（ソーシャルエンジニアリング）」の劇的な効率化である。これまで日本企業は、日本語というハイコンテクストかつ特殊な言語構造によって、海外からのフィッシング攻撃に対して一定の免疫を持っていた。いわゆる「ガラパゴスの防壁」である。不自然な日本語のメールは、従業員が直感的に排除できていた。

しかし、生成 AI の登場はこの防壁を完全に無効化した。現在の AI は、流暢な日本語を操るだけでなく、ターゲット企業の文脈や業界用語まで学習し、違和感のない文面を生成する。

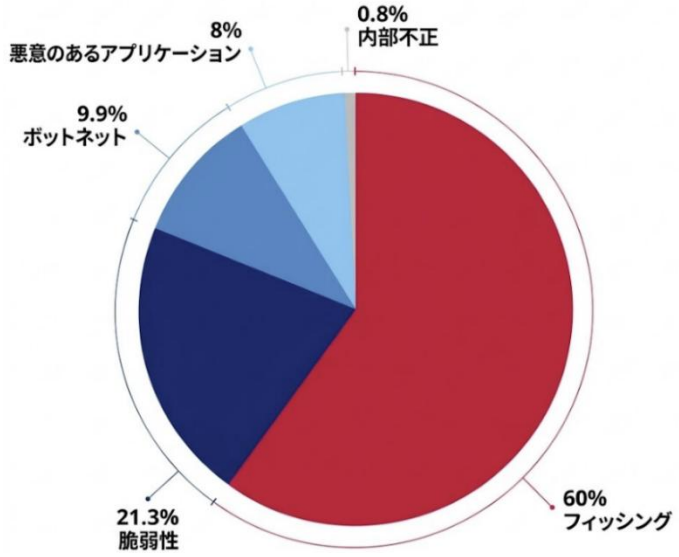
Heiding らの研究チーム（2024）の実証実験（注 2）によれば、AI が自動生成したフィッシングメールは、人間の専門家が時間をかけて作成したものと同等の開封率（約 54%）を記録している（図表 2）。さらに ENISA の分析では、侵入経路の約 60%がフィッシング等の「騙し」で占められている（図表 3）。従来、攻撃において「質（精巧さ）」と「量（攻撃回数）」はトレードオフの関係にあったが、AI はこの経済原則を破壊した。「人間並みの品質」を「ゼロコスト」で　「無限に量産」できるようになった今、従業員の注意喚起だけに頼る精神論的な防御策は、竹槍で爆撃機に挑むに等しく、早急なシステム的対策への転換が求められる。

図表 2　AI によるフィッシング作成能力の高さ



資料：Heiding, F., Lermen, S., Kao, A., Schneier, B., and Vishwanath, A. (2024 年 11 月 30 日). ″Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects″. arXiv:2412.00586.より筆者作成
*1：AI が作成したメール（54%）が、人間の専門家（54%）と同じ成功率を出していることを示す棒グラフ。
*2：対照群とは、特定の個人向けにカスタマイズされていない、既存の一般的なフィッシングメール（いわゆるバラマキ型メール）を送付されたグループを指す。AI や専門家による標的型攻撃の有効性を測定するための比較基準（ベースライン）として設けられた。

図表 3　侵入経路のシェア



資料：ENISA Threat Landscape 2025 より筆者作成
*1：攻撃の入り口の 60%がフィッシングであることを示す円グラフ。

(3)犯罪エコシステムの「市場化」とサプライチェーンの確立

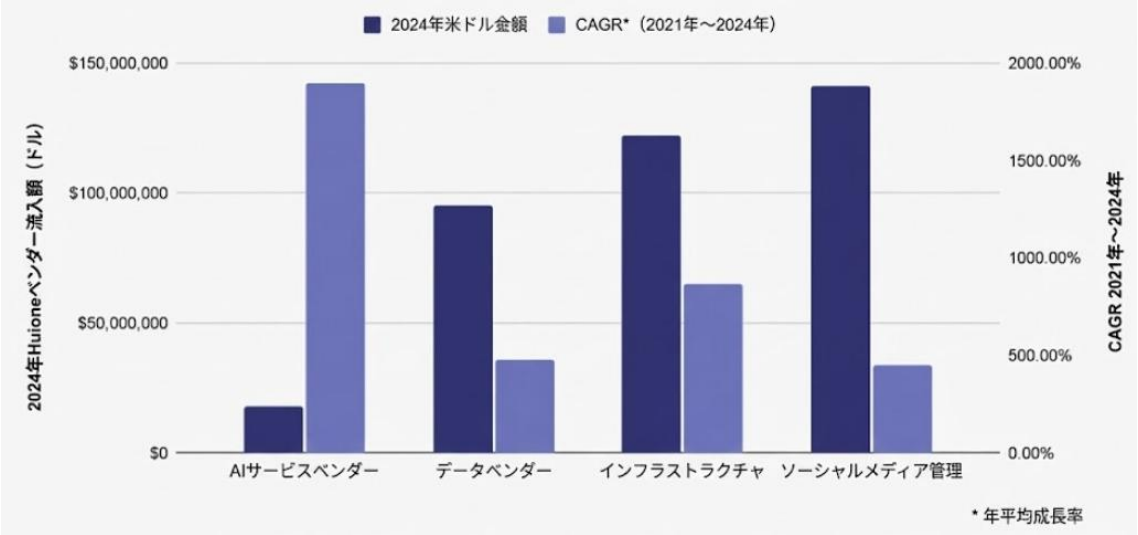
第三の要因は、犯罪インフラの高度な分業体制とエコシステムの成熟である。現在のサイバー犯罪は、単独犯による犯行ではなく、複雑なサプライチェーンによって支えられている。

Chainalysis の 2025 年版レポート（注 3）が指摘するように、「Huione Guarantee」のような犯罪者向けマーケットプレイスでは、標的企業のネットワークへの入り口を販売する「イニシャル・アクセス・ブローカー（IAB）」、偽サイト構築キットを提供するベンダー、そして盗んだ暗号資産を洗浄するマネーロンダリング業者がひしめき

合っている。これらはB2Bの SaaS 製品のようにカタログ化され、容易に売買されている。

特筆すべきは、これらのインフラ提供業者の収益成長率である（図表 4）。攻撃者は自らインフラを構築する手間をかけずとも、必要な機能を「部品」として調達し、組み合わせるだけで即座に事業を開始できる。この「犯罪のワンストップショップ化」は、正規のビジネス界におけるクラウドエコシステム形成と同様の進化を遂げており、攻撃コストを極限まで押し下げている。結果として、攻撃者は極めて低い損益分岐点で活動が可能となり、中小企業を含むあらゆる組織が標的となる構造が固定化されたのである。

図表 4　Huione 詐欺インフラ市場の収益規模と年平均成長率（2021～2024 年）



資料：Chainalysis 2025 Crypto Crime Report より筆者作成
*1：犯罪を支援するインフラ業者や AI ツール業者の売上が急増していることを示す棒グラフ。

3.技術戦から「経済戦争」へ

ここまで見てきたように、RaaS による攻撃能力の民主化、生成 AI による騙しの効率化、そして犯罪エコシステムの確立といった構造変化により、我々が直面しているのは、単なる技術的な不備やセキュリティホールの問題ではなく、「攻撃側の ROI（投資対効果）が高すぎる」という経済構造の問題である。つまり、極めて少ない投資で攻撃を持続的に行うことが可能な「産業」として成立してしまっているのだ。攻撃側が低コストで無限の試行回数を重ねられるのに対し、防御側がその都度高コストな対応を迫られる現状は、構造的に持続不可能である。この「非対称性」を解消しない限り、いくら最新のセキュリティ製品を導入しても、それは対症療法に過ぎない。

したがって、企業が検討すべき戦略は、防御の目的を「侵入をゼロにすること」から、ケンブリッジ大学のロス・アンダーソン教授が提唱する「セキュリティの経済学」（注 4）に基づき、「攻撃者のビジネスモデルを破綻させること」へと再定義するこ

とにある。具体的には、攻撃者の「コスト」を強制的に引き上げ、「利益」を不確実なものにするアプローチが求められる。

まず、多要素認証（MFA）やゼロトラスト・アーキテクチャの徹底は、単なるコンプライアンス対応ではなく、攻撃者に手間と時間を強いることで、割に合わない行為だと思わせるための「コストの壁」として機能する。特に、AIによる自動化攻撃が主流となる中、物理的なセキュリティキーや生体認証といった「AIが模倣できない物理的制約」を認証プロセスに組み込むことは、攻撃の自動化メリットを相殺し、コスト構造を悪化させる極めて有効な手段となる。

加えて、自社一社が堅牢であっても、取引先や海外拠点が「安価な侵入経路」として狙われれば意味をなさない。そのため、サプライチェーン全体でのセキュリティ水準の底上げ（全体最適）を主導し、攻撃者が容易に利益を得られる「弱い環」を排除することも不可欠である。

結論として、サイバーセキュリティはもはやIT部門の管轄事項ではなく、自社の事業継続性を守るための「経済戦争」であるといえる。本来であれば、国家レベルの政策介入によって攻撃者の市場メカニズムを破壊すべき課題ではある。しかし、マクロな解決を待つ間にも被害は拡大し続ける。だからこそ、ミクロな経済主体である企業は、自組織を「攻撃しても儲からない対象」へと変質させ、攻撃者の標的リストから外させるための経済合理的防衛策を講じなければならない。敵の収益構造を深く理解し、技術的な防御策を「攻撃者のROIをマイナスに追い込むための武器」として戦略的に配置する意思決定こそが、今、企業に求められているのである。

【注釈】

1. Boutemeur, J., Lella, I., Bakatsis, I., Chatzichristos, G., Foley, K., Leskinen, J., Otcenasek, J., and Ziolek, D. (2025年10月). "ENISA Threat Landscape 2025". European Union Agency for Cybersecurity (ENISA).
2. Heiding, F., Lermen, S., Kao, A., Schneier, B., and Vishwanath, A. (2024年11月30日). "Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects". arXiv:2412.00586.
3. Chainalysis. (2025年2月). "The 2025 Crypto Crime Report". Chainalysis.
4. Anderson, R. (2001年12月). "Why Information Security is Hard - An Economic Perspective". Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC).