2026 年 11 月 25 日　全 10 頁

AI 時代のサイバーレジリエンス

攻撃の「速度・質・量」の変化に、企業はどう備えるか

AI アナリティックリサーチ室　主任研究員　田邉 美穂
デジタルソリューション研究開発部　シニアセキュリティ・スペシャリスト　山崎 禎章

[要約]

- 国内でランサムウェア被害や不正アクセスによる情報漏洩が相次いでいる。こうした現状は、AI によるソフトウェアの脆弱性発見能力の向上とも無関係ではないと考えられる。この能力は開発元による問題の早期発見や修正に役立つ一方、攻撃者にも利用され得る。サイバー攻撃による被害は情報漏洩にとどまらず、業務の停止・遅延、長期の復旧作業、多額の費用負担など、被害企業の事業継続だけではなく、取引先を含むサプライチェーン全体に影響する経営上のリスクとなっている。

- 政府もサイバー攻撃を社会・経済活動の継続に関わるリスクと捉え、対応を強化している。2026 年 10 月には、官民連携の強化や、攻撃に使われるサーバー等を警察・自衛隊が無害化する措置などを柱とするサイバー対処能力強化法等の一部が施行された。さらに 11 月には、情報収集能力の強化に向けて同法の改正を検討するとともに、既知の脆弱性の修正などの基本対策、官民の情報共有、被害組織への支援などを盛り込んだサイバーセキュリティ緊急対策パッケージを取りまとめた。

- AI は、攻撃対象の情報収集、フィッシングメールや攻撃プログラムの作成、攻撃の実行など、サイバー攻撃のさまざまな場面で利用されていると考えられる。さらに、AI エージェントを悪用し、脆弱性の探索から侵入の試行までを自律的に進める攻撃も可能になりつつあり、攻撃の速度・質・量を変化させる可能性がある。他方、防御側でも、攻撃を受ける前の脆弱性診断や、攻撃を受けた際の監視・分析、サイバー攻撃への対応を支援する手段として AI の活用が期待されている。

- AI の進歩により、企業にとってサイバーセキュリティの重要性は一段と高まるだろう。企業は、AI が従来の基本対策を代替するものではないことを踏まえ、基本対策を着実に進めるとともに、システムの提供元や委託先を含め、攻撃を受けた際にも事業を継続・早期復旧できる体制を整える必要がある。その上で、自社の課題に応じて AI や外部サービスも適切に活用し、サイバーレジリエンスを高めることが求められる。

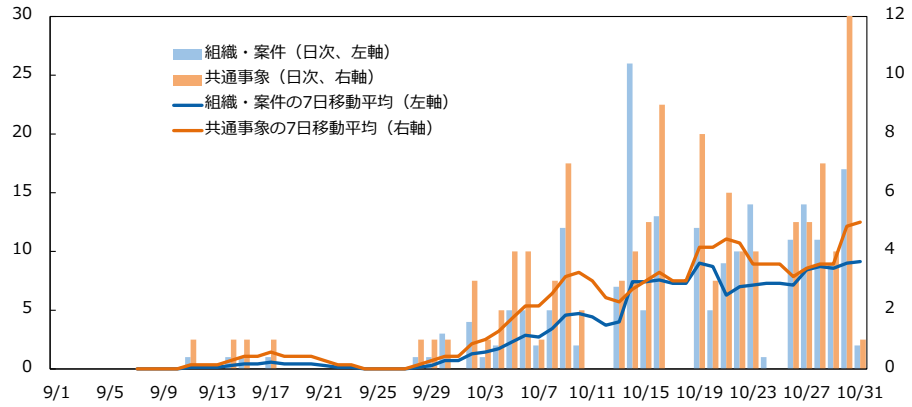
株式会社大和総研 丸の内オフィス　〒100-6756 東京都千代田区丸の内一丁目 9 番 1 号 グラントウキョウ ノースタワー
このレポートは投資勧誘を意図して提供するものではありません。このレポートの掲載情報は信頼できると考えられる情報源から作成しておりますが、その正確性、完全性を保証するものではありません。また、記載された意見や予測等は作成時点のものであり今後予告なく変更されることがあります。㈱大和総研と大和証券㈱は、㈱大和証券グループ本社を親会社とする大和証券グループの会社です。内容に関する一切の権利は㈱大和総研にあります。無断での複製・転載・転送等はご遠慮ください。

1. 相次ぐサイバー攻撃による被害とその影響[1]

増加するサイバー攻撃による被害と AI の影響

国内で、ランサムウェア被害[2]や不正アクセスによる情報漏洩が相次いでいる。警察庁によると、2026 年上半期に国内で報告されたランサムウェア被害は 123 件と、2020 年下半期の集計開始以降、半期として過去最多となった[3]。また直近では、一般向けサービスや業務用システムへの不正アクセスによって、大量の個人情報が漏洩する事案も目立つ。2026 年 9 月以降に日本経済新聞 電子版で新たに報道された日本国内の個人情報流出件数を、組織・案件ごとに集計した結果、9 月の 9 件に対し、10 月は 204 件と急増した（**図表 1**）。さらに複数の組織にまたがる同一事案を 1 件にまとめた「共通事象」で数え直しても、9 月の 7 件に対し、10 月は 108 件と 15 倍を超える。

図表 1 2026 年 9 月以降に報道された日本国内の個人情報流出件数の推移（日次、単位：件）



（注）期間は 2026 年 9 月 1 日～10 月 31 日。日本経済新聞 電子版「個人情報流出」トピックで報じられた国内の企業、公的機関、団体が対象。組織・案件は組織と案件の組み合わせで、流出の疑いを含む。共通事象は、共通して使うサービスや委託先への攻撃など、複数の組織にまたがる案件を 1 件として数えた値。7 日移動平均は当日を含む後方 7 日間の平均。日付は記事の公開日（同一案件は最初の報道日）で、攻撃の発生日ではない。集計方法の詳細は、新田尭之「個人情報流出はどの程度増えたのか？」（大和総研コラム、2026 年 10 月 30 日）を参照。
（出所）日本経済新聞 電子版より大和総研作成

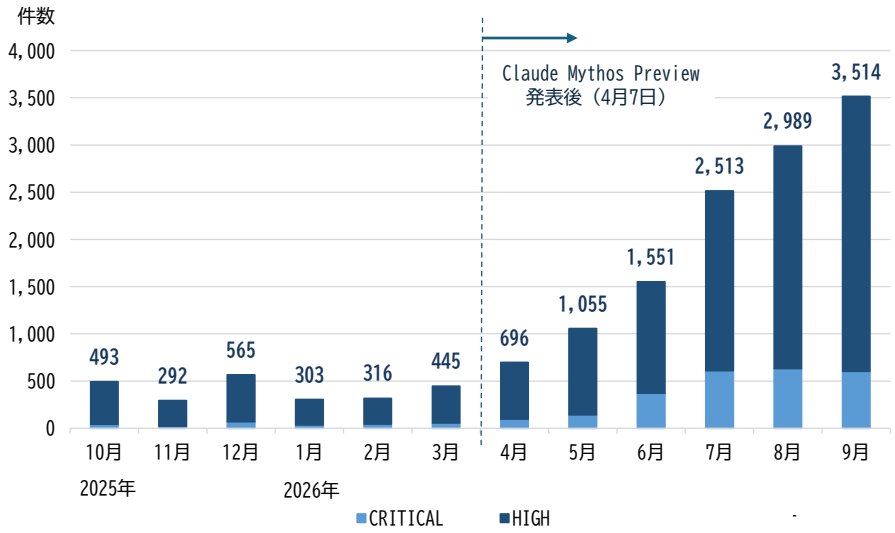
こうした現状には、AI によるソフトウェアの脆弱性発見能力の向上も無関係ではないと考えられる。AI による脆弱性発見能力の向上は、開発元が未知の問題を早期に把握し、修正する上で有用である。一方、攻撃者が同じ能力を使えば、修正される前の脆弱性を見つけて攻撃に悪用できる。攻撃者が脆弱性を発見し、攻撃に悪用するまでの時間が短くなれば、企業側の対応が間に合わない事態が生じやすくなる。

2026 年 4 月に米 Anthropic が、サイバーセキュリティ分野で高い能力を持つ汎用言語モデル「Claude Mythos Preview」を発表した。その後も、米国や中国などの複数の企業から、高度な

[1] 本稿では、主に第 1 章および第 4 章を田邉、主に第 2 章および第 3 章を山崎が担当。
[2] ランサムウェアとは、企業などのシステムに侵入してデータを暗号化したり盗み出したりし、データの復旧や情報の非公開と引き換えに金銭を要求するサイバー攻撃を指す。
[3] 警察庁サイバー警察局「令和 8 年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和 8 年 9 月）

サイバーセキュリティ能力を持つ AI モデルが相次いで公表されている。米国の AI 動向研究機関 Epoch AI の集計によると、ソフトウェアやハードウェアに関わる主要な 21 の企業・団体が公表した深刻度の高いソフトウェア・ハードウェアの脆弱性の件数は、これらのモデルの登場時期と重なるように大きく増加している（**図表 2**）。

図表 2 ソフトウェア・ハードウェアの脆弱性の報告件数（月別、単位：件）



（注）主要なソフトウェア・ハードウェア企業およびオープンソース団体 21 組織が、公表された脆弱性情報を識別・整理し、共有する国際的な取り組みである CVE Program を通じて公表した脆弱性情報（CVE レコード）のうち、CVSS（脆弱性の深刻度を評価する指標）に基づく深刻度が、「High」（7.0～8.9）または「Critical」（9.0～10.0）と評価されたものを公表月別に集計。
（出所）Epoch AI “Cyber vulnerabilities”, updated Oct 25, 2026 より大和総研作成

脆弱性発見能力をはじめとする AI の性能向上がサイバー攻撃にもたらす変化については、第 2 章で詳しく整理する。

サイバー攻撃による企業活動への影響も深刻化

サイバー攻撃では、個人情報や機密情報の漏洩に目が向きやすい。しかし、影響はそれだけにとどまらない。ランサムウェアなどによりシステムやデータが利用できなくなれば、受発注、製造、販売、物流、顧客対応など、幅広い業務が停止・遅延する可能性がある。サイバー攻撃の影響は、情報管理上の問題だけでなく、企業が重要な業務を継続できるかという経営上の問題にも及ぶ。

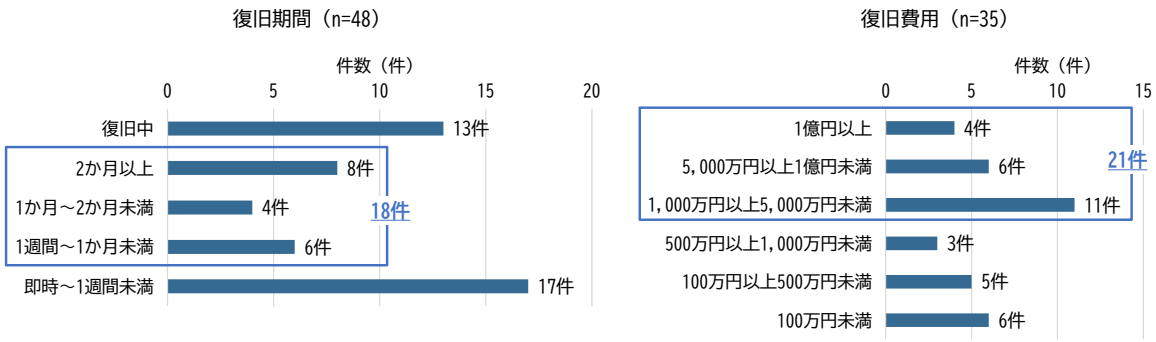
被害からの復旧には、長い時間を要する場合もある。警察庁が 2026 年上半期のランサムウェア被害を調査したところ、復旧期間について有効回答が得られた 48 件のうち、18 件（37.5%）は 1 週間以上を要し、13 件（27.1%）は調査時点でも復旧中だった（**図表 3 左**）。また、日本情報経済社会推進協会（JIPDEC）が 2026 年 1 月に実施した「企業 IT 利活用動向調査 2026」では、ランサムウェアの感染被害を経験した企業のうち、システムやデータの復旧に成功した割合は半数を下回る。さらに、復旧に成功した企業では約 7 割が 1 カ月以内に復旧している一方、復旧できなかった企業では約 4 割が断念するまでに 1 カ月超を費やしている。この結果は、長

期間復旧作業を続けても、復旧に至らない場合があることを示している[4]。これら二つの調査は、調査対象や回答方法が異なるため単純な比較はできないが、復旧が長期に及び得る点は共通している。

復旧には相応の費用もかかる。前述の警察庁の調査では、調査・復旧に要した費用について有効回答が得られた 35 件のうち、21 件（60.0%）が総額 1,000 万円以上を要したと回答している。このうち、1 億円以上の回答も 4 件あり、全有効回答の 11.4%を占めた（**図表 3 右**）。これらは被害に伴う調査・復旧費用であり、業務停止による売上機会の喪失や顧客・取引先への対応、信用の低下などを含めれば、企業が被る損失は調査で把握された金額を上回る可能性がある。

さらに、影響は被害を受けた企業の中だけに収まるとは限らない。業務を支える子会社や委託先、取引先、クラウドサービスなどが攻撃を受ければ、取引関係を通じて複数の企業へ波及する可能性がある。KPMG ジャパンが日本経済新聞社と共同で行った調査では、サイバー攻撃による業務上の被害が生じた経路として国内の委託先・取引先が最も多かった。また、国内の委託先・取引先を経由した攻撃の有無を把握できていない企業は３割弱に上り、委託先のセキュリティ対策を継続的に把握する仕組みに課題があることが示されている[5]。サイバー攻撃は、被害企業の情報システム上の問題にとどまらず、取引先を含むサプライチェーン全体に影響を及ぼし得る経営上のリスクとして捉える必要がある。

図表 3 2026 年上半期のランサムウェア被害からの復旧期間・費用



（出所）警察庁サイバー警察局「令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和 8 年 9 月）、p.11 より大和総研作成

政府もサイバー攻撃への対応を強化

こうした中、政府もサイバー攻撃への対応を強化している。2026 年 10 月 1 日には、能動的サイバー防御（サイバー攻撃の兆候を把握し、重大な被害の未然防止や拡大防止を図る取り組み）の実現に向けた「サイバー対処能力強化法」および「同整備法」（サイバー対処能力強化

[4] 一般財団法人日本情報経済社会推進協会「『企業 IT 利活用動向調査 2026』から見る日本企業の DX、AI 活用、ランサムウェア被害の実態（集計結果および分析レポート）」（2026 年 4 月 16 日公表、2026 年 4 月 23 日修正版、調査協力：株式会社アイ・ティ・アール）

[5] KPMG ジャパン「サイバーセキュリティサーベイ 2026」（2026 年 6 月 3 日）

法等）の一部が施行された[6]。同法等による取り組みは、①官民連携の強化、②通信情報の利用、③アクセス・無害化措置の三つを柱とし、このうち今回施行されたのは①と③に関する規定である。②の通信情報の利用は 2027 年秋以降に開始される予定だ。

①官民連携では、電力、鉄道、通信、金融などの基幹インフラ事業者に対し、重要なシステムに関係する機器の製品名などの資産情報の届出や、不正アクセスや悪意のあるプログラムの実行など、一定のサイバーインシデントの報告を求める。その上で政府は、基幹インフラ事業者から届け出られた資産情報と、未公表のものを含む脆弱性情報を突き合わせ、該当する事業者に速やかに注意喚起を行う。また、政府と民間で脅威情報を共有するための協議会も設置された。

③アクセス・無害化措置では、サイバー攻撃によって重大な危害が発生するおそれがある場合など一定の要件の下で、警察や自衛隊が攻撃に使用されているサーバーなどにアクセスし、不正なプログラムの停止・削除などを行うことが可能になった。

こうした制度の運用が始まる一方、政府は、日本を標的としたサイバー攻撃の兆候や被害をより迅速に把握するため、情報収集能力をさらに強化する必要があるとして、同法の改正を検討する方針だ[7]。

さらに、政府は 2026 年 11 月 6 日、相次ぐサイバー攻撃や情報漏洩を受け、「サイバーセキュリティ緊急対策パッケージ」を取りまとめた[8]。政府は同パッケージで、昨今の情報漏洩事案には、既知の脆弱性の放置や設定の不備など、自組織や委託先の基本的な対策が不十分だった例が多いと指摘した。さらに、AI の進歩によって、こうした隙が短時間かつ大規模に突かれるようになったとの認識も示している。その上で、①「AI も活用した基本的な対策の徹底」、②「情報収集・集約、捜査・分析体制の強化」、③「サイバー攻撃への対処の戦略的実施」、④「被害者支援・被害拡大防止策の強化」を柱に掲げた。AI を活用した脆弱性診断や、セキュリティベンダー、クラウド事業者、先端 AI 企業などとの情報共有、官民の専門人材による被害組織への支援などを通じ、社会全体でサイバー攻撃の被害を抑え、早期の対応・復旧につなげる方針である。

サイバー攻撃を社会・経済活動の継続に関わるリスクとして捉え、社会全体で備える動きも国内外で進んでいる。政府は、サイバー攻撃などによる大規模な停電や通信障害、断水などが長期化し、国民生活に深刻な影響を及ぼす場合には、災害対策基本法上の「災害」として対応する方針を示した[9]。海外でも、英国政府が 2026 年 10 月、自然災害からサイバー攻撃まで幅広

---

[6] 内閣官房国家サイバー統括室、内閣府政策統括官（サイバー安全保障担当）「サイバー対処能力強化法等の施行について」（2026 年 9 月）

[7] 首相官邸「サイバーセキュリティに関する関係閣僚会議」（令和 8 年 11 月 6 日）

[8] サイバーセキュリティに関する関係閣僚会議決定「サイバーセキュリティ緊急対策パッケージ」（令和 8 年 11 月 6 日）。同パッケージには、高性能 AI を活用した脆弱性診断、「官民サイバー救援隊（仮称）」等による被害組織への支援、「サイバーセキュリティお助け隊サービス」に復旧・バックアップ支援メニューの追加などが盛り込まれた。

[9] 社会的影響が特に深刻な大規模インフラ障害への対応に係る関係府省連絡会議決定「社会的影響が特に深刻な大規模インフラ障害への対応の基本的考え方について」（令和 7 年 7 月）

い緊急事態に備え、国民に 3 日分の食料や水などを準備するよう促す「Be Ready」キャンペーンを開始したことが話題となった[10]。サイバー攻撃を、自然災害などと同様に社会で備えるべき緊急事態の一つとして位置付けた例といえる。

2. AI がサイバー攻撃をどう変えるのか

サイバー攻撃における AI 利用の現状

昨今のサイバー攻撃による被害の増加を踏まえると、サイバー攻撃における AI の利用は進んでいると考えて間違いないだろう。AI は、攻撃対象に関する情報収集、フィッシングメールの作成、攻撃プログラムの作成、脆弱性の探索、横展開、攻撃の実行など、攻撃の準備から実行に至るまでのさまざまな場面で利用されていると考えられる。攻撃者は AI を利用することで、言語の壁などから従来は狙いにくかった対象も攻撃できるようになった。さらに、従来よりも短時間で準備を進め、より多くの対象に攻撃を仕掛けることが可能になっている。

最近、大きく次元が変わったと考えられるのが、AI エージェントがサイバー攻撃に利用される事例である。LLM（大規模言語モデル）を用いて脆弱性診断・ペネトレーションテスト[11]を自動化する、ARTEX や Strix といった AI エージェント型ツールが登場している。これらのツールが攻撃者に悪用され、実際のサイバー攻撃に用いられたという報道がある[12][13]。これらのツールは脆弱性診断・ペネトレーションテストを行うために攻撃的なスキルが組み込まれており、対象となるシステムの情報やどのようなテストを行うかといった情報を与えると、脆弱性の探索、侵入方法の検討、試行などを自律的に進める。本来の目的に反して、許可を得た診断対象ではなく無許可の攻撃対象のシステム情報を与えると、そのままツールが攻撃を実行するという流れだ。

ただし、実際のサイバー攻撃について、攻撃者が AI を使ったかどうかを被害者の立場から証明することは基本的には難しい。攻撃者が利用していたツールの管理画面が誤って公開されている場合を除けば、攻撃のパターンから AI が使われたかどうかを推測するしかできない。また、AI を使った攻撃であっても、AI 特有の対処方法があるわけではないため、攻撃に AI が使われているかどうかは本質的な問題ではないともいえる点は注意が必要である。

---

[10] GOV.UK Campaigns “Be Ready”, last accessed November 24, 2026; Cabinet Office and The Rt Hon Dan Jarvis MBE MP “Households encouraged to take small, simple steps to stay prepared in an emergency”, October 22, 2026.

[11] ペネトレーションテスト（侵入テスト）とは、実際の攻撃者に近い手法でシステムへの侵入を試み、セキュリティ上の弱点や侵入の可能性を検証するテストを指す。

[12] CrowdStrike, “Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance”, October 7, 2026.

[13] Gambit Security, “AI Agents Are Hacking Online Retailers for $25 a Company”, September 22, 2026.

AI が変える攻撃の「速度・質・量」

AI がサイバー攻撃に与える影響は、**「速度・質・量」**の三つの観点で整理できる（**図表 4**）。

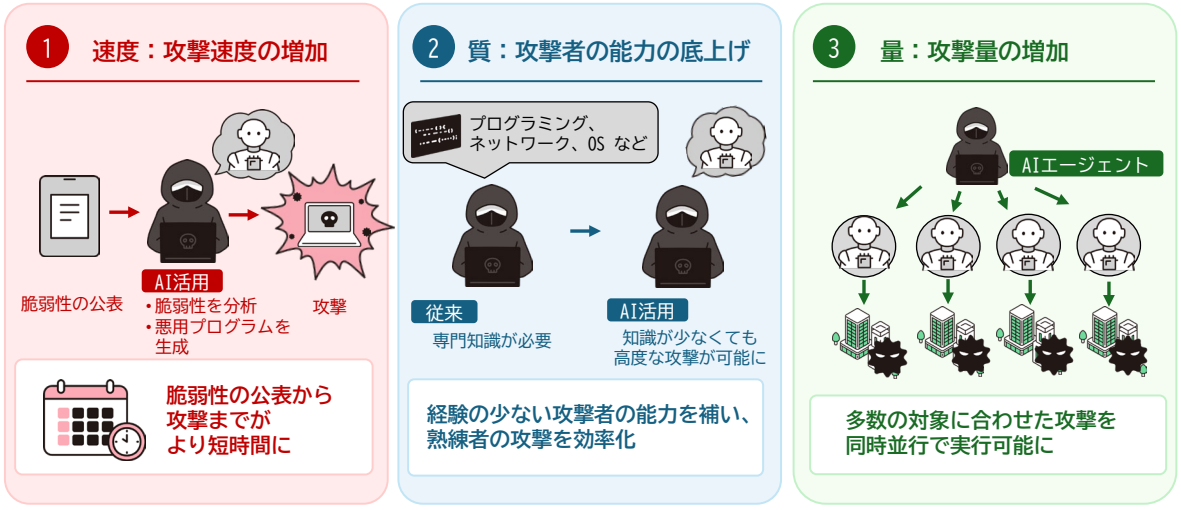
第一は、**攻撃速度の増加**である。ソフトウェアの脆弱性が公表されると、攻撃者は公開情報や脆弱性を修正する更新プログラム（パッチ）の内容を分析し、その脆弱性を悪用するプログラムを生成することができる。AI が攻撃者に悪用されると、脆弱性公表から攻撃への転用までの時間が短縮されることが考えられる。その結果、企業側が脆弱性を修正するまでに与えられる時間も短くなってしまう。

第二は、**攻撃者の能力の底上げ**、いわば攻撃の質の変化である。従来、高度な攻撃には、プログラミング、ネットワーク、OS などさまざまな領域について一定の専門知識が必要だった。AI が調査やコード生成を支援することで、経験の少ない攻撃者でも、従来と同等レベルのサイバー攻撃を行うことが可能になった。

第三は、**攻撃量の増加**である。AI エージェントを悪用したサイバー攻撃では、複数のエージェントを同時並行で稼働させることで、多数の企業やシステムに対して、一斉に攻撃を行うことが可能になった。従来は企業ごとにシステムの特性が異なることが一斉攻撃の障壁となっていたが、AI によって対象に合わせて攻撃を調整して仕掛けることが容易となり、この障壁は低下している。

もっとも、AI によって攻撃者側が完全に有利になるとも限らない点は触れておきたい。経験の少ない攻撃者が AI を利用した場合に、多くの痕跡を残すことがあり、身元を隠すための対策が不十分であることもある。多数の痕跡から従来よりも攻撃者を追跡することが容易となる可能性もある。

図表 4 AI がサイバー攻撃に与える影響



（出所）大和総研作成（イラストはソコスト https://soco-st.com/）

3. 防御側の考え方と AI の活用

企業に求められる基本的な考え方

サイバー攻撃への対応では、攻撃を完全に防ぐことだけを目指すのではなく、攻撃を受けることも前提に、被害を抑えながら重要な事業やサービスを継続し、早期に復旧できるよう備える「サイバーレジリエンス」の考え方が重視されてきた[14]。具体的には、脆弱性への対応や認証の強化などによって侵入されにくくするとともに、侵入された場合にも被害が広がらないよう検知・対応し、バックアップなどを活用して早期に復旧できる体制を整えることが基本となる。

こうした基本的な考え方は、AI の登場によって大きく変わるものではない。一方、攻撃側で AI の活用が進み、攻撃の速度や質、量が変化すれば、防御側にもそれに応じた対応が求められる。

防御への AI 利用とは

攻撃側での AI の活用が進む一方で、防御側でも AI を利用する動きが広がっている。セキュリティ領域での AI の利用は「攻撃を受ける前の対策」と「攻撃を受けた際の対応支援」の二つに分けられる（**図表 5**）。

一つ目は、AI を利用した脆弱性診断やペネトレーションテストである。AI を利用した脆弱性診断では、AI にソースコードやシステムの情報を与えて分析させることによって、脆弱性の候補を網羅的に抽出する。AI を利用したペネトレーションテストは、AI に実際の攻撃者に近い形でシステムへの侵入を行わせて、そのシステムで特に有効な攻撃手法を調べるという方法である。攻撃者側が頻繁に脆弱性探索や侵入を試みている現状からすると、防御側も先回りしてこれらを定期的に行い、事前に対策していくことが必要になっていくと考えられる。

二つ目は、セキュリティ監視やインシデント対応での利用である。企業が管理する機器・システムからは日々大量のログやセキュリティ警告が発生する。従来の SOC（セキュリティ・オペレーション・センター）による、サイバー攻撃の兆候の監視・分析や対応に加えて、AI にもこれらの分析を行わせるといった形である。例えば、同じ利用者による通常とは異なる場所からのログインなど、人間の SOC 担当者では気付きにくい攻撃パターンなども発見することが期待できる。また、過去事例や外部からの脅威情報を照合して、自社が攻撃されていないかを発見する際にも AI と対話しながら評価を行うといった利用方法が考えられる。これらは AI を用いた SOC である「AI-SOC」や脅威の兆候を能動的に探索する「脅威ハンティング」と呼ばれる活用方法である。

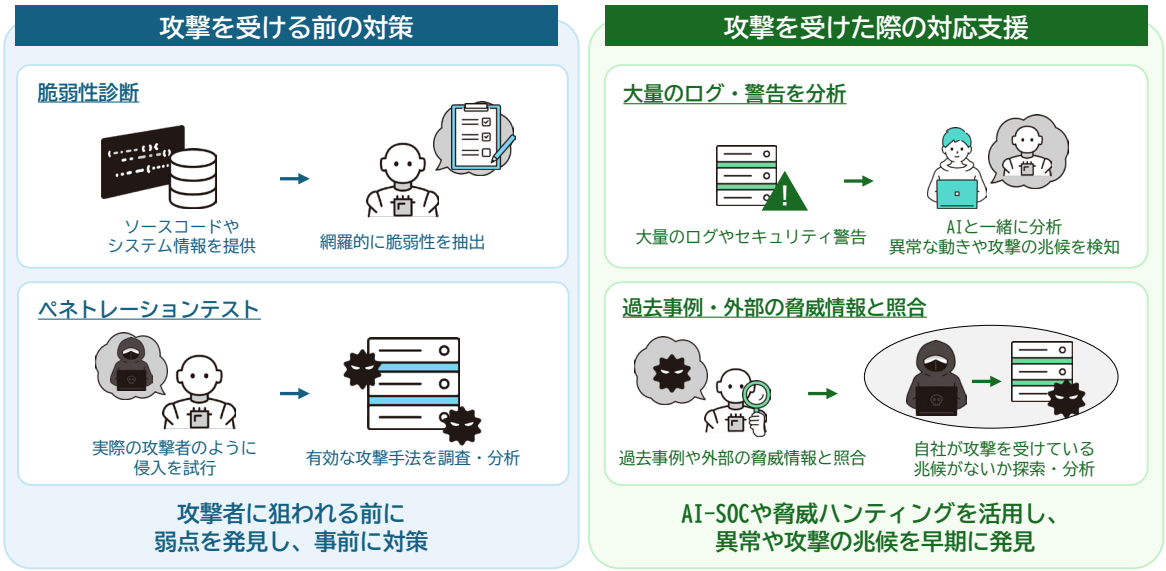
---

[14] サイバーセキュリティ戦略本部「サイバーセキュリティ 2026（2025 年度年次報告・2026 年度年次計画）」（令和 8 年 7 月 31 日）においても、「幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上」が政策の柱の一つに掲げられている。

ただし、AI が脆弱性や異常を検知したとしても、その妥当性を検証しなければならない点には注意が必要である。特に、セキュリティ監視においてAIの判断が誤っていた場合、正常な業務を停止させることにもつながるため、慎重な評価が求められる。

AI は、資産管理、脆弱性対応、認証強化、バックアップといった従来の基本対策を代替するものではない、という点にも触れておきたい。AI によるセキュリティ強化は従来の対策の上に成り立つものであり、これらが不十分な状態では、AI が問題を発見できたとしても早期の対応を行うことは難しい。そのため、まずは従来の対策が十分にできていない領域を優先して対応し、その上でAIの導入を検討すべきである。

図表 5 防御側での AI 利用イメージ



（出所）大和総研作成（イラストはソコスト https://soco-st.com/）

4. 企業は基本対策を土台に対応力の強化を

AI によってサイバー攻撃が高度化・高速化・大規模化する可能性がある中、企業には、防御、検知、対応、復旧に要する時間を短縮することが求められる。前章でみたように、防御にAIを活用することで、セキュリティ担当者による判断や対応を迅速化できる可能性があるものの、AI 自体は従来の基本対策を代替するものではない。まずは、守るべきシステムやデータと対応・復旧の優先順位を明確にし、基本対策を着実に進める必要がある。

特に、専門人材や予算が限られる中小企業では、高度な監視・対応体制を自社だけで構築するのは難しい。独立行政法人情報処理推進機構（IPA）は、中小企業がはじめに取り組むべき基本的な対策として、①OS やソフトウェアを常に最新の状態に保つ、②ウイルス対策ソフトを導入する、③パスワードを強化する、④共有設定を見直す、⑤バックアップを取る、⑥脅威や

攻撃の手口を知る、という「情報セキュリティ 6 か条」を示している[15]。また、政府は、サイバーセキュリティ緊急対策パッケージにおいて、中小企業向けの「サイバーセキュリティお助け隊サービス[16]」として、復旧やバックアップなどの支援を行う方針を示している。中小企業は、まずは実施可能な基本対策から着実に取り組むとともに、利用可能な外部サービスや今後具体化される支援策も念頭に置きつつ、自社の対応体制を段階的に整えていくことが重要だろう。

自社内の対策に加え、システムの提供元や委託先を含めたリスク管理も欠かせない。業務システムやクラウドサービスの提供元、システムの運用委託先などでサイバー攻撃や情報漏洩、システム障害が発生した場合も、自社の事業に影響を及ぼしかねない。サービスの選定時だけでなく、利用開始後も提供元や委託先のセキュリティ対策を継続的に把握し、問題発生時の報告や対応、復旧に関する役割分担を確認しておく必要がある。委託元が委託先に求める対策水準を共通基準で示し、その実施状況を確認する政府の「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）」が、2026 年度末頃から開始される予定である[17]。提供元や委託先が評価を取得している場合、その評価結果も対策状況を把握する材料の一つとなろう。

AI の進歩によってサイバー攻撃が高度化・高速化・大規模化する中、企業にとってサイバーセキュリティの重要性は一層高まるだろう。こうした変化は、自社の対策や対応体制を見直す機会にもなり得る。攻撃に AI が使われているかどうかにかかわらず、企業に求められる基本的な備えが大きく変わるわけではない。基本対策を着実に進めた上で、AI の特性や限界を理解し、自社の課題に応じて適切に活用することで、攻撃を受けても事業を継続し、早期に復旧できるサイバーレジリエンスを高めていくことが求められる。

以上

[15] 独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン」（2016 年 11 月 15 日公開、2026 年 9 月 30 日最終更新）

[16] 中小企業に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージにまとめた、民間の事業者から提供されるサービス。詳細は独立行政法人情報処理推進機構（IPA）「サイバーセキュリティお助け隊サービス ユーザー向けサイト」を参照。

[17] 経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）」（2026 年 11 月 9 日最終閲覧）。また、大橋 哲行「SCS 評価制度の『★』、問われるのは"取得"より"維持"：体制・人材・運用が、取引の信頼を左右する」（大和総研レポート、2026 年 9 月 30 日）も参考にされたい。