

AI による攻撃も、通る道は同じ——入口・アカウント・痕跡の点検で備える

攻める AI への備えも、社内の AI の統制も、1枚の点検表で確かめる。新規上場31社で「攻撃者の AI」に触れた会社は0社。

① 攻撃者が AI を使う

AI で変わるのは、速さと費用です。公開済みの脆弱性を攻撃コードに変える作業は速くなり（Google・2026年9月）、修正済みのブラウザの脆弱性を突く攻撃コードを、AI が約20ドルで組んだ報告もあります（Anthropic・2026年9月）。AI がほぼ全工程を進めた実例も報告され始めましたが、最初の侵入は、インターネットに公開された、既知の脆弱性を抱えたサービスからでした（Microsoft・2026年10月）。変わらないのは、入口、アカウント、痕跡です。

国は、重要インフラと金融機関から手を打っています。2026年10月に施行された重要インフラの統一基準は、攻撃者に AI が悪用され、脆弱性の発見から悪用までが短くなることを踏まえて、パッチ適用の方針を確立するように求めています。金融機関には、金融庁・日本銀行の要請（2026年5月22日）があり、資産の把握や特権 ID への多要素認証など6つの対策を挙げています。同じ要請には、次の一文もあります。

「一方で、英国 AISI（AI 安全性評価機関）の報告書によれば、現時点ではフロンティア AI は、十分に防御された IT システムに対しては、攻撃を達成できるとは言えないと報告されている。」

要請は、この一文を踏まえたうえで、上の対策を求めています。それ以外の一般の企業に、AI を使った攻撃への備えを求める国の指針は、当社が現時点で確かめた範囲では見当たりません。国の検討は続いています（経済産業省のワーキンググループほか）。一方、AI を使った攻撃の試みは、国内でもすでに観測されています（JPCERT/CC・2026年10月）。検討が整うまでの間、この1枚と点検表が、各社の備えの一助になれば幸いです。

当社の調べでは、2026年に新規上場した31社の「事業等のリスク」の章で、AI に触れた会社は14社（45%）、攻撃者による AI の利用に触れた会社は0社でした（記載は提出時点のもので、書いていないことは対策をしていないことを意味しません）。当社の点検表47問のうち14問は、この要請が挙げる対策と重なります。重要インフラでも金融機関でもない会社も、同じ対策から始められます。

② 防御に AI を使う

攻撃が安く速くなった以上、守りも年1回の点検では追いつきません。国も重要インフラに、脅威の検知や脆弱性の発見に高性能 AI を活用するよう勧めています（2026年5月）。ただし防御の AI は、管理者に近い権限を持ちます。だから②も、次の③と同じ6要素で確かめます。当社は、AI に任せるのを「見つける・知らせる・直す案を出す」までとし、取り消せない操作は人が承認する形を勧めます。

③ 自社の AI 利用を統制する

AI を、人のアカウントや委託先と同じように台帳に載せて管理します。統制の要素は6つです。専用の ID、必要最小限の権限、操作ログ、人による承認、停止の権限と手順、そして外部 AI サービスを委託先として扱うこと。31社のうち、自社の AI 利用のリスクを書いたのは3社でした。当社の点検表（2026年10月版）では、この6要素を「社内で使う AI」の6問として加えました。

攻める AI への備えも、社内の AI の統制も、1枚の点検表で確かめられます

攻める AI への備えは、国の注意喚起などを具体的な問いにした点検表で、社外から見えている入口／ログイン・アカウント・管理者の権限／侵入に気づく・対応する／大事なデータの守り方／経営・委託先・社外との連絡の5つの群・47問で。社内の AI は6つ目の群の6問で。結果を選ぶと優先度と経営向けの理由が自動で出ます。委託先に送る質問票にもなります。その後も継続して確かめるなら、証跡付きで測り続けられる当社の診断が支援します。

入口は A-14（悪用されている脆弱性）、アカウントは B-1（管理者の多要素認証）、痕跡は C-1（身に覚えのないファイル）。御社は、この3問に今日答えられますか。点検表（無料）と診断＝
<https://www.secuoi.com/#checklist>