ChatGPT

シャドーAIの問題点と対応策の実務分析レポート

エグゼクティブサマリー

本レポートでは、「シャドーAI（野良AI）」を**組織が正式に承認していない、または監督していないAIツール・AI機能・AI連携の業務利用**として整理する。この現象は、従来のシャドーITが生成AI・AIエージェント・AI内蔵SaaSへ拡張したものであり、ブラウザーからの一般公開チャットボット利用、個人端末からの持ち込み、SaaSのAI機能の無断有効化、部門単位の自己調達、社内ツールから外部AI APIをたたく無許可実装など、多様な経路で発生する。NCSCはシャドーITを「組織内で業務目的に使われている未知の資産」と定義し、個人クラウド・未承認サービス・無許可デバイスなどを典型例として挙げている。IBMもシャドーAIを「IT部門の正式承認や監督なしに従業員やエンドユーザーがAIツールを使うこと」と定義している。 [1]

指定記事の主要主張である「企業の7割超が対策できず」は、日経クロステック記事そのものの公開スニペットと、より直接的にはGartner Japanの2026年6月18日公表データによって強く裏づけられる。Gartnerによれば、**国内企業の75%が部門主導の未承認寄りの生成AI利用を何らかの形で認めている一方、43%がシャドーAIを把握できず、30%が把握していても有効対策を取れておらず、合計73%が有効管理できていない**。これは記事タイトルの「7割超」と整合する。さらにGartnerは、対応の方向性として「完全な管理」から「責任ある活用」への移行、すなわち**全面禁止ではなく、可視化・審査・承認・統制の分業モデル**を推奨している。 [2]

リスクは大きく、情報漏えい、個人情報保護法・GDPR等の法令違反、知的財産や営業秘密の流出、誤情報による業務品質低下、プロンプトインジェクション等のサイバーリスク、そして監査証跡やeDiscovery不備による内部統制上の問題に分かれる。日本の個人情報保護委員会は、生成AIサービスに個人情報を含むプロンプトを入力する際は**利用目的の範囲内かを確認し、個人データが応答以外の目的で扱われるなら法違反の可能性があるため、機械学習に利用しないこと等を十分確認すること**を明示している。EU側でもEDPBとイタリアGaranteがAIと個人データ処理に強い問題意識を示しており、規制・執行の現実性は高い。 [3]

原因は、単なる「従業員のルール違反」ではない。Microsoft/LinkedInの2024 Work Trend Indexでは、**世界の知識労働者の75%が仕事でAIを使い、AI利用者の78%が自前のAIを職場に持ち込んでいる**。同調査では**60%のリーダーが自組織にはAI実装の計画・ビジョンが不足している**と回答している。NCSCも、シャドーITは悪意よりも「仕事を終わらせるために公式ツールが足りない」ことから生じると説明する。学術的にも、Klotzらのシステマティックレビューは、**ITシステムの不足、IT部門の遅さ、コスト期待、認知不足、制約不足**を主要因として整理している。 [4]

したがって、実務上の最適解は「禁止」ではなく、**承認済み代替手段を先に用意した上で、可視化・データ統制・役割分担・契約審査・教育・監査を一体運用すること**である。具体的には、プロキシ/CASB/SaaS管理による検出、DLPとブラウザー制御による送信防止、SSOやPrivate Marketplace等による承認済みアプリ管理、ポリシーと契約条項の整備、AI-IRSを踏まえたインシデント対応、そして職種別教育・認定である。NIST AI RMF、NIST CSF 2.0、IPA、AISI、ANSSI、NCSCの方向性はこの点でかなり収れんしている。 [5]

指定記事の要約と検証

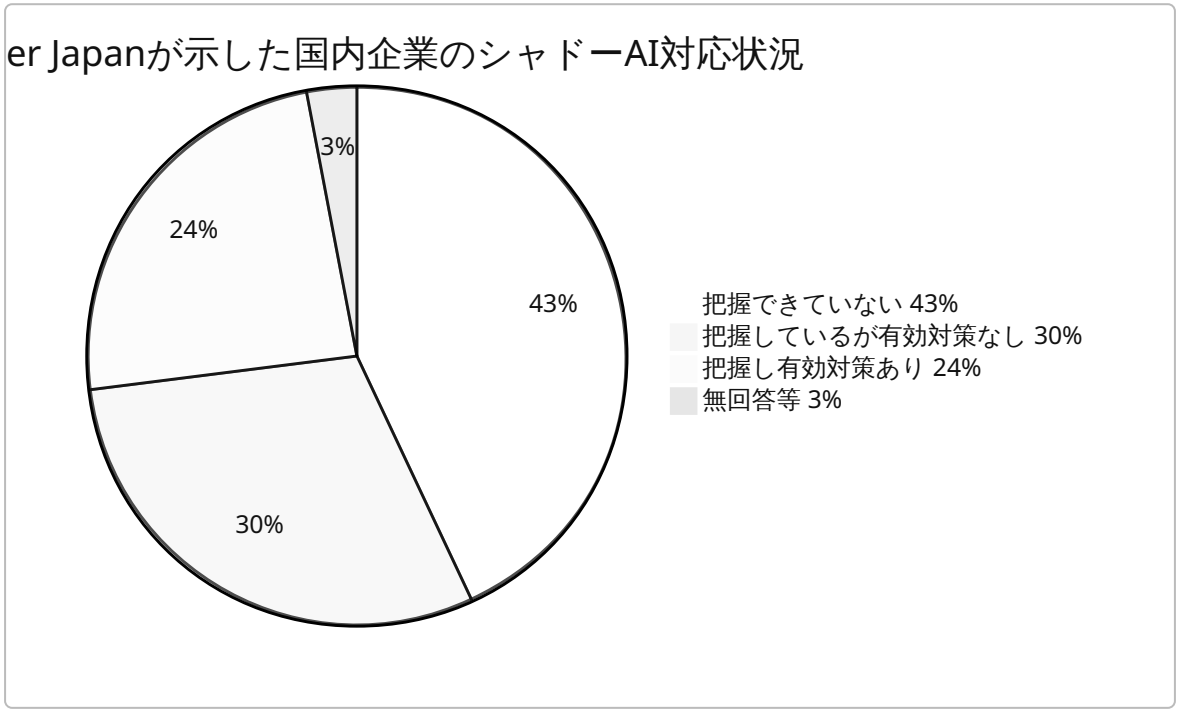
指定記事として確認できたのは、日経クロステック2026年6月26日公開、馬場貴子氏による記事の**原題「企業の7割超がシャドーAI対策できず、放置で情報漏洩・法令違反のリスクも」**である。検索環境では本文全文を直接確認できなかったため、**公開タイトル、日経クロステック公式Xの告知スニペット、及び同記事が参照した可能性が非常に高いGartner Japanの一次発表**で検証した。記事URLとして確認できたものは次の通り

である。
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062200211/ [6]

日経クロステック公式Xの公開スニペットには、記事要旨として**「シャドーAIの対策を進める企業が増えてきていますが、『全面禁止』は正解…」**という文脈が出ている。これは、本文の論点が単なる危険喚起ではなく、**禁止一辺倒の限界と、運用設計の必要性**にあることを示していると解釈できる。もっとも、本文全文を閲覧できていないため、この点は**公開スニペットに基づく限定的確認**である。 [7]

記事の中核命題を一次情報で照合すると、Gartner Japanの2026年6月18日発表は非常に近い。Gartnerは、**75%の国内企業が部門主導の生成AI利用を何らかの条件付きまたは自由に容認**している一方で、**43%がシャドーAIを把握できず、30%が把握していても有効な対策を取れていない**と公表した。合計73%であり、記事タイトルの「7割超が対策できず」をほぼそのまま裏づける。加えて、**有効対策を取れている企業は24%**にとどまる。記事がもし「企業の7割超が対策できていない」と表現したなら、その統計的基盤は十分に妥当である。 [8]

さらに、記事のもう一つの論点である「全面禁止は正解ではない」も、Gartnerの提言と整合する。Gartnerは企業に対し、**AIを“IT部門が一貫管理する全社標準AI”“部門ごとに審査・運用するAI”“教育と認定を前提に認める個人利用AI”の3類型に分け、採用時審査・利用中モニタリング・定期棚卸しの3ステップを回す**ことを勧めている。これは、**禁止よりも、分類・可視化・責任分担・再評価**を重視する実装論である。Microsoftの調査でも、日本で**BYOAIが78%**に達しているため、現場実態としても一律禁止は守られにくい。 [9]



上図はGartner Japanの2026年6月発表に基づく概念図である。記事の「7割超」が、**43%＋30%=73%**という一次データで裏づけられていることを可視化した。 [8]

検証結果を要約すると、指定記事の主要論点は次のように評価できる。

記事の主要主張	一次情報による検証	判断
企業の7割超が対策できず	Gartner Japanは73%がシャドーAIを有効管理できていないと公表。 [8]	**妥当**
情報漏洩・法令違反のリスク	PPCは個人データ入力時の法違反可能性を明示。Gartnerも機密情報・個人情報流出、法令違反、脆弱性、評判毀損を主要リスクとして列挙。 [10]	**妥当**
全面禁止は正解ではない	Gartnerは「完全な管理」から「責任ある活用」への移行と分業モデルを提言。Microsoft調査ではBYOAIが既に広がっており、禁止だけでは実効性が低い。 [11]	**妥当**
利用実態の可視化が必要	Gartnerはクラウド通信監視による可視化と定期棚卸しを重視。NCSCも影の資産は資産管理外であり、まず発見・管理対象化が必要とする。 [12]	**妥当**

シャドーAIの定義と発生メカニズム

本レポートでは、シャドーAIを**「組織の正式承認・監督・リスク評価・契約審査・監査設計の外で使われるAI」**と定義する。IBMはシャドーAIを、**IT部門の正式な承認や監督なしに従業員やエンドユーザーがAIツールやアプリケーションを使うこと**と定義している。Gartnerは、日本企業向けには**「企業が正式に承認していないAIツール／サービス」**という表現を用いる。NCSCのシャドーIT定義を合わせると、シャドーAIは単に「未承認のAI SaaS」だけでなく、**未知のデバイス、個人クラウド、無許可のAPI接続、社内で勝手に立てたAI連携**も含むと考えるのが実務的である。 [13]

発生経路は、利用者視点では単純だが、統制側から見ると非常に見えにくい。第一に、**個人端末・ブラウザー・モバイルアプリ**から一般公開チャットボットを使う経路がある。第二に、**SaaSやブラウザー拡張のAI機能をユーザーが勝手に有効化**する経路がある。第三に、**部門がクレジットカード等でAI SaaSを自己調達**する経路がある。第四に、**社内ツールやRPA、ノーコード基盤から外部AI APIへ接続**する経路がある。第五に、**ベンダー製SaaSに後からAI機能が追加され、管理者が把握しないまま利用が始まる**経路がある。NCSCは未承認メッセージング、個人クラウド、無管理の開発環境やコード保管先を典型例として挙げており、IBMはAIチャットボット、ML分析、マーケティング自動化、可視化ツールを実例としている。 [1]

技術的特徴として重要なのは、**導入摩擦の低さ、データ流通の見えにくさ、確率的出力、外部依存性**である。NISTのGenerative AI Profileは、生成AIリスクが**LLM、クラウドベースサービス、調達・取得**のような横断的活動に関わると説明している。IBMも、多くのAIアプリケーションが**SaaSとして提供され、ITやセキュリティ部門を経由せずに即座に導入される**と指摘する。さらにPPCは、入力した個人情報が**機械学習に利用され得る**こと、出力には**不正確な内容が含まれ得る**こと、利用規約やプライバシーポリシーの確認が要ることを明示している。つまり、シャドーAIは「便利な外部検索箱」ではなく、**外部事業者・外部モデル・外部保存先・外部規約**を伴う情報処理基盤である。 [14]

実務上は、次の整理が有用である。

類型	典型的な発生経路	具体例	技術的に見えにくい理由
個人端末由来	私物PC/スマホ、個人ブラウザー、モバイルアプリ	公開チャットボットへの業務文書貼付け	端末管理・ブラウザー監視の対象外になりやすい。 [1]
SaaS機能由来	既存SaaSのAI機能を勝手に有効化	文書要約、メール草案、会議要約	既存SaaSの一機能として紛れ、アプリ追加として見えにくい。 [15]

類型	典型的な発生経路	具体例	技術的に見えにくい理由
部門調達由来	部門カード決済、無料プラン、試用版	AIライティング、AI分析、AI翻訳	契約・購買審査を通らず、資産台帳に載りにくい。 16
チャットボット由来	Web入力・ファイル添付・会話履歴	顧客対応文面作成、技術質問、議事録化	入力内容が外部送信され、保存・学習・再利用条件がツールごとに異なる。 17
社内ツール無許可連携	APIキー埋め込み、RPA/ノーコード、社内Bot	API経由で社内DBやチケットシステムと連携	一見すると社内ツールだが、背後で外部モデルや外部APIを利用している。 18
開発現場由来	IDE拡張、コード生成、無管理リポジトリ	生成AIコーディング、コードレビュー支援	ソースコード・設計情報・シークレットが混在しやすい。 19

リスク分類と事例

シャドーAIのリスクは、従来のシャドーITのリスクを引き継ぎつつ、**「入力した情報が外部モデルへ渡る」「出力がもっともらしく誤る」「エージェント化で権限行使まで進む」**というAI特有の性質により増幅される。IPAは、組織導入におけるリスクとして**機密情報流出、ハルシネーション、マルウェア生成、著作権侵害、個人情報保護法・GDPR抵触**などを整理している。NISTのGenAI Profileも、**Data Privacy、Information Integrity、Information Security、Intellectual Property**を生成AI固有または増幅された主要リスクとして列挙している。 20

以下では、ユーザー指定の分類に沿って、公開事例または公開執行例を付して整理する。なお**影響度は、法的制裁の重さ、事業継続への影響、復旧難易度、再発防止コストを踏まえた実務上の概算評価**である。

リスク分類	典型シナリオ	国内外の事例・公開例	影響度	主な根拠
情報漏洩	社員が公開AIへ設計書、議事録、顧客情報、コード断片を貼り付ける	Samsungは2023年、社員が機密コードをアップロードした事案を受け、ChatGPT等の利用を一時制限した。GoogleやAppleも機密情報入力を控えるよう社内警告を出した。	**高**	21
個人情報保護法・GDPR等の法令違反	本人同意や利用目的整理なしに個人データを外部AIへ送る	PPCは、個人データが応答以外の目的で扱われる場合は法違反の可能性があると注意喚起し、OpenAIにも注意喚起を実施。GaranteはChatGPTに対し一時的利用制限・その後の改善要求を実施した。EDPBもAIモデルとGDPRの関係でケース別評価と説明責任を重視した。	**高**	22
知的財産・機密漏洩	ソースコード、営業秘密、著作物、設計ノウハウを外部AIへ投入する	Samsungの事例は機密コード流出の典型。文化庁はAIと著作権の関係について、関係者別チェックリストとガイダンスを公表し、権利侵害リスク低減措置の必要性を示している。	**高**	23

リスク分類	典型シナリオ	国内外の事例・公開例	影響度	主な根拠
業務品質・誤情報	AI出力を検証せずそのまま顧客対応・法務・企画へ流用する	Mata v. Aviancaでは、ChatGPTが生成した架空判例を弁護士が提出し、米裁判所が制裁を科した。PPCも、生成AIの出力には不正確な個人情報が含まれるリスクを指摘している。	**中**	24
サイバーセキュリティ	プロンプトインジェクション、データ抜き取り、マルウェア支援、権限昇格	OWASPはPrompt InjectionとSensitive Information DisclosureをLLM/GenAIの上位リスクに位置付ける。Microsoftは間接プロンプトインジェクションの現実的脅威を説明しており、EchoLeak研究はMicrosoft 365 Copilotでの機密情報流出実証を報告した。	**高**	25
コンプライアンス・監査上の問題	誰が何をAIに入力し、何が出力され、どこへ保存されたか追跡できない	Microsoft PurviewがChatGPT Enterprise向けにAuditing、eDiscovery、Communication Compliance等を提供している事実は、企業利用で監査・証跡が必須であることを示す。加えて、米国ではAIチャット記録が捜査令状の対象となり、必ずしも秘匿特権が認められないことが示された。	**中**	26

補足すると、**国内の公開一次情報では、企業名入りの大規模「シャドーAI起因漏えい」事案よりも、PPCの注意喚起やガイドライン整備の方が先行している**。一方、海外では規制執行、裁判所制裁、セキュリティ研究開示まで出そろっており、日本企業が「まだ大きな事故が見えていないから後回しでよい」と判断するのは危険である、というのが本調査から導ける実務的含意である。これは上記公開事例の分布に基づく推論である。 27

原因分析

シャドーAIの原因を一言で言えば、**「現場の需要が、IT・法務・セキュリティの供給能力を上回っている」**ことである。NCSCは、シャドーITは通常悪意ではなく、**従業員が公認ツールや公認プロセスで仕事を終えられないため**に生じると述べる。Microsoft/LinkedInも、社員が仕事の量とスピードに押され、会社の準備不足の中で自前AIを持ち込んでいると示している。つまり、原因分析では「モラルの低さ」より、**業務設計・承認設計・教育設計・アクセス設計の未整備**を重く見るべきである。 28

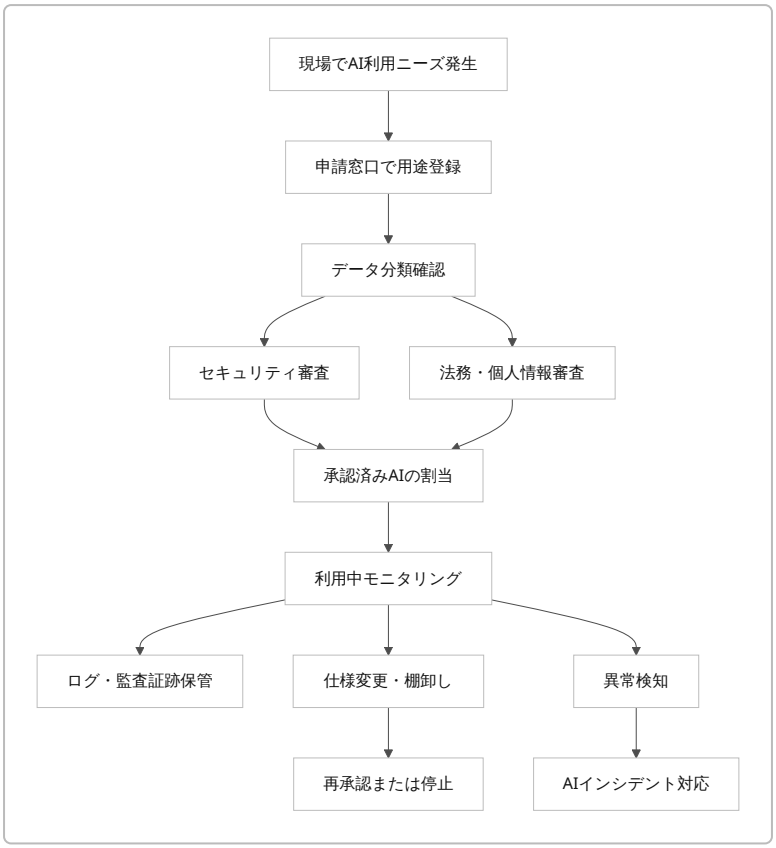
原因	具体像	根拠となる調査・論文・報告書
利便性・生産性優先	忙しい現場が「まず使えるもの」を選び、承認を後回しにする	Microsoftは75%が仕事でAIを使い、78%がBYOAI、背景に仕事量とスピード圧力があると報告。IBMも生産性向上・迅速な問題解決がシャドーAI普及要因とする。 29
ITガバナンスの欠如	AI利用方針や責任分担がなく、現場が独自判断する	Gartnerは73%が有効管理できておらず、Microsoftは60%のリーダーがAI実装の計画・ビジョン不足を懸念。Reuters/Nikkei Research調査では日本企業の4割超がAI活用計画なしと報じられた。 30

原因	具体像	根拠となる調査・論文・報告書
既存システム・承認プロセスの不足	公認ツールが遅い、機能不足、外部共有しにくい	NCSCはストレージ不足、外部共有不可、必要サービスへのアクセス不足、承認の遅いリクエストプロセスを代表要因に挙げる。KlotzらはIT system shortcomings、IT organization slowness、long development/purchase timesを主要因として整理した。 [31]
教育不足・認知不足	従業員が、何が禁止で何が危険かを知らない	KlotzらはAwareness lackとして「IT標準違反者の80%が自分が違反していると知らない」研究を引用。MicrosoftではAI訓練を受けた利用者は39%にすぎない。PPCも利用規約・プライバシーポリシー確認を求めている。 [32]
アクセス管理・可視性の不備	誰がどのAIにアクセスし、何を送ったか分からない	CiscoはAIシステムとデータセットのアクセス制御で**72%が堅牢な態勢に届いていない**と報告。NCSCは未知資産である以上、組織は「何を守るべきか」を十分理解できないとする。 [33]
組織文化の問題	申告すると怒られるため、利用が地下化する	NCSCは、非難・処罰型の文化では従業員がシャドーITを報告しなくなり、可視性がさらに下がると明言する。USENIXの事例研究も、従業員の認識・リスク理解・組織との関係性が行動に影響すると示す。 [34]

原因をさらに実務向けに言い換えると、次の三層で捉えると分かりやすい。第一層は**需要側の圧力**で、現場は速さ・便利さ・成果を求める。第二層は**供給側の不足**で、IT部門が承認済みAIや迅速な審査窓口を用意できていない。第三層は**統制側の遅れ**で、法務・セキュリティ・監査がAI特有のデータ流れや証跡要件をルール化できていない。この三層が重なると、社員は「一時的な例外」ではなく「常態的な抜け道」として野良AIを使うようになる。 [35]

対応策の比較と実装

対応方針の基本は、**全面禁止ではなく、可視化→分類→承認→監視→見直し**のループを作ることだ。これはGartnerの「責任ある活用」への移行、NIST AI RMFの**Govern / Map / Measure / Manage**、NIST CSF 2.0の**Govern / Identify / Protect / Detect / Respond / Recover**、AISIの**観測性と制御性**、ANSSIの**事前リスク分析とDevSecOps**に共通する。言い換えると、シャドーAI対策は単独製品導入ではなく、**AIガバナンス運用の設計問題**である。 [36]



上図は、Gartnerの採用時審査・利用中モニタリング・定期棚卸し、AISIの観測性/制御性、NIST CSFの継続的運用を実務ワークフローに落とした推奨形である。 [37]

対策比較表

対策	実装手順	コスト感	利点	限界	参考
検出・可視化	プロキシ/ファイアウォール/クラウドログを収集し、CASBやSaaS管理でアプリ利用を棚卸し。新規・高リスクAIアプリを自動検出し、台帳化する。	**中**	まず「何が使われているか」が分かる。禁止より先に必要な基盤。	個人端末やモバイル通信は取りこぼす。ログ品質に依存。	NCSCはCASB、SASE、UEM、ネットワークスキャナを技術的緩和策に挙げる。Microsoft Defender for Cloud AppsもCloud DiscoveryでShadow IT発見・リスク分析・unsanctionが可能としている。 [38]
DLP・ブラウザー制御	先に機密区分と検出パターンを定義し、AIアプリ向けにコピー/貼付け/アップロード/送信を制御。まずブラウザーDLPから始め、段階的に拡張する。	**中**	機密データ送信を直接抑止できる。ユーザー影響を限定しやすい。	誤検知・業務阻害の調整が必要。SaaSごとの実装差あり。	Microsoft Purview DLPは機密情報保護の計画、検知、調査のライフサイクルを示し、Edge for Business向けCloud Apps DLPを提供する。 [39]

対策	実装手順	コスト感	利点	限界	参考
アクセス制御	承認済みAIはSSO/MFA必須にし、未承認アプリはプロキシ/ファイアウォールで制御。必要に応じてPrivate Marketplaceや承認済みカタログを用いる。	**中〜高**	野良AIより先に「公式に使えるAI」を作れる。調達統制にも効く。	現場ニーズに追いつかないと抜け道が残る。	NCSCは強いネットワークアクセス制御を推奨。Google Cloud Private Marketplaceは検証済み製品のみ調達・配備できる仕組みを提供。 15
ポリシー策定と分業モデル	「禁止データ」「許可用途」「個人利用条件」「承認手順」「記録保持」「違反時対応」を定義。IT、セキュリティ、法務、人事、現場責任者の役割を明記する。	**低**	低コストで始められ、教育・契約・監査の土台になる。	文書だけでは守られない。承認済み代替手段がないと形骸化。	Gartnerは分業モデルと3類型整理を提言。METI「AI事業者ガイドライン」はAIガバナンスの統一的指針を示す。IPAは組織導入ガイドラインと中小企業向け規程ひな形を提供。 40
契約条項・法務審査	新規AI/SaaS契約時に、学習利用の有無、保存期間、データ所在、再委託、監査権、削除、秘密保持、知財帰属、ログ提供可否を審査する。個人データ用途ならDPIA相当評価も行う。	**中**	後から「規約を読んでいなかった」を防げる。対外説明に強い。	無料ツールや個人利用は契約統制しにくい。	PPCは利用規約・プライバシーポリシー確認を求める。EDPBはAIモデルにおけるGDPR適用でケース別評価と記録保持の重要性を示す。文化庁はAIと著作権のチェックリストを公表。 41
監査・インシデント対応	AI利用ログ、会話記録、承認履歴、モデル変更履歴を保持。異常な送信、プロンプトインジェクション、幻覚起因事故に対する通報・封じ込め・復旧手順を整備する。	**中〜高**	事故時の説明責任と再発防止に不可欠。監査・訴訟対応にも有効。	コンシューマー向けAIでは十分なログや管理機能がない場合がある。	AISIはAI-IRSで観測性と制御性を中核に据える。NIST CSF 2.0はRespond/Recoverまで含めた継続運用を要求。Microsoft PurviewはAuditingやeDiscoveryの管理機能を提供。 42
従業員教育・認定	全社向け基本研修と、開発・法務・営業・人事など職種別研修を分ける。承認済みAIの使い方、禁則データ、出力検証、引用・著作権、顧客対応時の注意を明文化し、修了者のみ一部機能を開放する。	**低〜中**	最も汎用性が高い。禁止だけでは難しい「判断の質」を上げる。	単発研修では効果が薄い。運用中の継続教育が必要。	Gartnerは教育と認定による責任ある実践者の育成を必須条件とする。Microsoftでは訓練不足が顕著。Klotzらは認知不足を主要因として示した。 43

対策	実装手順	コスト感	利点	限界	参考
リスク評価フレームワーク	NIST AI RMFでユースケースをGovern/Map/Measure/Manageし、NIST CSFで技術統制へ接続。AISIのAI-IRSで運用時の観測性・制御性を補い、ANSSIの推奨でサプライチェーンと外部データも評価する。	**中**	単発対策を体系化でき、部門別の例外管理にも耐える。	小規模組織にはやや重い。運用設計に人手が要る。	44

これらの中で、**最初に効くのは「可視化」と「承認済み代替手段の提供」**である。NCSCが繰り返す通り、シャドーIT/AIは多くの場合、社員の悪意ではなく、必要な機能が不足しているときに生じる。したがって、最初から締め付けだけを強めるより、**社内で使ってよいAI、入れてはいけないデータ、申請すれば使える追加AI**を明確にした方が実効性が高い。 16

一方で、技術統制だけでも不十分である。PPCやEDPBの観点では、**個人データがどこに送られ、何の目的で処理され、保存・学習に使われるのか**を説明できなければ、法的に危うい。文化庁の観点では、**生成物の商用利用可否だけでなく、入力元・出力物・権利帰属・類似性**を含めた著作権判断が必要になる。つまり、シャドーAI対策は、情報システム部門だけで閉じるテーマではなく、**法務・個情・知財・監査を含む企業横断統制**として扱う必要がある。 45

実務チェックリストと主要参照先

以下は、一般企業を想定した実務向けチェックリストである。業種固有規制がある金融・医療・公共・教育では、個人情報・記録管理・説明責任の強度を一段引き上げるべきである。優先度は**高・中・低**で示す。

期間	優先度	実施項目	主担当	到達目標
短期	**高**	生成AI・AI機能の利用実態を棚卸しする	情シス/CISO	主なAIアプリ、利用部門、データ流れを把握する
短期	**高**	「入力禁止データ」を決める	情シス・法務・個情・事業部	個人データ、顧客秘密、未公開財務、ソースコード等の禁則を明文化する
短期	**高**	暫定ポリシーを出す	経営・CIO・CISO	全面禁止ではなく、許容/禁止/申請制を区別する
短期	**高**	承認済みAIの一次リストを作る	情シス・調達	現場が「使ってよいもの」をすぐ選べる状態にする
短期	**中**	全社員向け15〜30分の初期研修を実施	人事・セキュリティ	禁則データ、出力検証、外部共有の危険を周知する
中期	**高**	プロキシ/CASB/SaaS管理でShadow AI検出を始める	情シス/SOC	新規AIアプリ検出とリスクスコアリングを実施する

期間	優先度	実施項目	主担当	到達目標
中期	**高**	ブラウザーDLPまたはアップロード制御を導入	情シス・セキュリティ	高機密データの送信を抑止・警告できるようにする
中期	**高**	契約審査テンプレートを整備	法務・調達・個情	学習利用、保存、削除、監査権、再委託、データ所在を確認できるようにする
中期	**中**	申請フローを簡素化	CIO室・情シス	「遅いから野良AIを使う」を減らす
中期	**中**	ログ・監査証跡・保存方針を定義	監査・情シス・法務	後追い調査と説明責任に耐える状態を作る
長期	**高**	AIガバナンス委員会を常設	経営・CIO・CISO・法務・監査・現場	仕様変更や新規AI導入を継続的に審査する
長期	**高**	NIST AI RMF/CSFとAI-IRSを統合運用	情シス・セキュリティ・監査	リスク評価から事故対応まで一本化する
長期	**中**	職種別認定制度を導入	人事・各部門	開発、営業、法務、人事などで必要なAI利用水準を差別化する
長期	**中**	四半期ごとに棚卸し・再承認	情シス・資産管理・監査	「一度承認したら放置」を防ぐ
長期	**中**	サプライチェーン・外部モデル評価を実施	調達・セキュリティ	外部モデル、外部データ、外部ライブラリの信頼性を確認する

最後に、実務で優先的に参照すべき主要ソースを列挙する。ユーザー要請に合わせ、主要URLを明記する。

- 指定記事 日経クロステック: `https://xtech.nikkei.com/atcl/nxt/column/18/00989/062200211/` [6]
- Gartner Japan「国内企業の『シャドーAI』対応における新たな指針」: `https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20260618-aibs-shadow-ai` [8]
- 個人情報保護委員会「生成AIサービスの利用に関する注意喚起等」: `https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/` [46]
- PPC 別添PDF「生成AIサービスの利用に関する注意喚起等」: `https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf` [47]
- 経済産業省「AI事業者ガイドライン 第1.2版」: `https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf` [48]
- IPA「テキスト生成AIの導入・運用ガイドライン」: `https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/generative-ai-guideline.html` [49]
- IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」: `https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf` [50]
- AISI「AIインシデントレスポンス・アプローチブック」: `https://aisi.go.jp/assets/pdf/ai-irs_v1.0_ja.pdf` [51]
- NIST AI RMF Generative AI Profile: `https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf` [52]

- NIST Cybersecurity Framework 2.0: `https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf` [53]
- ENISA「Artificial Intelligence Cybersecurity Challenges」: `https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges` [54]
- NCSC「Shadow IT guidance」: `https://www.ncsc.gov.uk/guidance/shadow-it` [55]
- 文化庁「AIと著作権について」: `https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html` [56]
- EDPB Opinion 28/2024 on AI models and GDPR: `https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en` [57]
- Garante main decisions archive: `https://www.garanteprivacy.it/web/garante-privacy-en/main-decisions` [58]
- ANSSI「Security recommendations for a generative AI system」: `https://messervices.cyber.gouv.fr/guides/en-security-recommendations-generative-ai-system` [59]

総括すると、シャドーAIは「AI利用が進んだ結果の例外現象」ではなく、**AI活用が本格化した組織でほぼ必ず生じる運用課題**である。指定記事の警鐘は、Gartnerの73%未管理という数字、PPCの法的注意喚起、NIST/IPA/AISIのガバナンス枠組みによって、十分に補強される。実務上の最優先は、**発見できていないAI利用を見える化し、現場が使える承認済み代替手段を同時に整えること**である。ここを外すと、禁止は地下化を招き、導入促進は放任に堕する。シャドーAI対策の本質は、AIの利用を止めることではなく、**責任ある利用へと変換する統制設計**にある。 [60]

---

[1] [15] [16] [18] [28] [31] [34] [35] [38] [55] https://www.ncsc.gov.uk/guidance/shadow-it
https://www.ncsc.gov.uk/guidance/shadow-it

[2] [8] [9] [11] [12] [30] [36] [37] [40] [43] [60] https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20260618-aibs-shadow-ai
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20260618-aibs-shadow-ai

[3] [10] [17] [22] [27] [41] [45] [47] https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf
https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

[4] [29] https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part
https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part

[5] https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-shadow-it
https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-shadow-it

[6] https://qiita.com/pitopito/items/35ba71bd2cf2155b3ea4
https://qiita.com/pitopito/items/35ba71bd2cf2155b3ea4

[7] https://x.com/NIKKEIxTECH/status/2070299911942541527
https://x.com/NIKKEIxTECH/status/2070299911942541527

[13] https://www.ibm.com/jp-ja/think/topics/shadow-ai
https://www.ibm.com/jp-ja/think/topics/shadow-ai

[14] [44] [52] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[19] https://www.reuters.com/technology/apple-restricts-use-chatgpt-wsj-2023-05-18/
https://www.reuters.com/technology/apple-restricts-use-chatgpt-wsj-2023-05-18/

20 https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003spo-att/f55m8k0000003svn.pdf
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003spo-att/f55m8k0000003svn.pdf

21 23 https://www.reuters.com/technology/chatgpt-fever-spreads-us-workplace-sounding-alarm-some-2023-08-11/
https://www.reuters.com/technology/chatgpt-fever-spreads-us-workplace-sounding-alarm-some-2023-08-11/

24 https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/
https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/

25 https://genai.owasp.org/llmrisk/llm01-prompt-injection/
https://genai.owasp.org/llmrisk/llm01-prompt-injection/

26 https://learn.microsoft.com/en-us/purview/ai-chatgpt-enterprise
https://learn.microsoft.com/en-us/purview/ai-chatgpt-enterprise

32 https://ijispm.sciencesphere.org/archive/ijispm-070102.pdf
https://ijispm.sciencesphere.org/archive/ijispm-070102.pdf

33 https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/2024-m11/documents/cisco-ai-readiness-index.pdf
https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/2024-m11/documents/cisco-ai-readiness-index.pdf

39 https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

42 https://aisi.go.jp/activity/activity_security/260109/
https://aisi.go.jp/activity/activity_security/260109/

46 https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/
https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/

48 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf

49 https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/generative-ai-guideline.html
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/generative-ai-guideline.html

50 https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf

51 https://aisi.go.jp/assets/pdf/ai-irs_v1.0_ja.pdf
https://aisi.go.jp/assets/pdf/ai-irs_v1.0_ja.pdf

53 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

54 https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

56 https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html
https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html

57 https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en
https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en

58 https://www.garanteprivacy.it/web/garante-privacy-en/main-decisions
https://www.garanteprivacy.it/web/garante-privacy-en/main-decisions

59 https://messervices.cyber.gouv.fr/guides/en-security-recommendations-generative-ai-system
https://messervices.cyber.gouv.fr/guides/en-security-recommendations-generative-ai-system