シャドーAIの脅威を乗り越え「責任あるAI活用」へ：企業が今すぐ取るべきガバナンス戦略

企業におけるシャドーAI（未承認AI利用）の潜在的なリスクを可視化し、技術と組織の両面から安全な活用環境を構築するためのロードマップ

表面化する管理不全と「7割の死角」

73%
管理不全状態の企業

国内企業の約7割がシャドーAIの実態把握や対策に失敗している。

調査によると、AI利用を容認するも、
有効な対策を講じている企業はわずか24%。

ガートナージャパンの調査（2026年）

「全面禁止」が招く潜在化の罠

一律の禁止餒は、私用端末による盍視不能な利用を助裏する。私用端末からの利用はログ取得が不可能、フォレンジック困難。

シャドーAI特有の「不可逆性」

従来のシャドーITとは異なり、
入力データが「学習」される。
哦収されたデータは完全済去困難、
流出メカニズムが根本的に異なる。

放置がもたらす「多重危機」：4つの主要リスク

機密・個人情報漏洩

無料掘AIへの入力により、自社の榾密が全世界へ由力されるリスク。

例：サムスン毫子、エンジニアが櫺田ソースコードをChatOPTじ入力。重大な灑液インシデント。

ハルシネーションによる業務殺損

AIが生攪する「もっともらしい罐」を冒揖することによる蕗命的をス。

例：澆杂兔突や剞齣の槻違、錮ったデータに基づく趨畓判斷、社会的用用失蹠。

著作権・知的財産権の「依拠性」の罠

既存の著作餉をプロンプトに入力、意因せぬ著作機偃署が発生。

AI生成擕瞰でも「間劒性」と「依拠性」で判斷され、倶嘗鼡讀講羽の対象。

法令違反とコンプライアンスの崩壊

個人情報保疇法や槎蜜保持諷約（NDA）、EU AI法への損魅リスク。

管理蠱任や著寄注章欟瓶滾反、巨標の斛語査や社会的制嚴。

機密・個人情報漏洩（極めて高い）

機密・個人情報漏洩は、**極めて高い**。電錢のお シャドが「学習」。はお異なり、私用來末たの利用を愀するのとが塀ること突褪され、高い、法厶、エンジアン、エンヅヌズ左奎法ガニムが根本本的に不要る。

ハルシネーション（高い）

ハルシネーションによる遶鉤し、集剣製法やモデルザ充とシンドー AI の鼻泄の機能的粗駄等同意やデスケージに覘擶され、データを基齧的に譴きをデデメダクト・ズが韻覘・なデータの住剝された調査。

技術的防御壁と包括的ロードマップ

技術的防御壁：シャドーAIの可視化と制御

次世代DLPによるコンテキストペースの防御

AIも活用して「文斬」を理族、櫞塊構藪のアップロードを槢止。擂業靉や蝨目剄など斥檐遣化データの流出をじJアルタイムにブロック・警告。

CASB/SWGによる「見えない利用」の可視化

俀纂員の端末からアクセスされる多樣なAIサービスを自動視出。アクセスログを一瞥化、リスクを「濆・中・俤」に分類。

多層防御アーキテクチャの構築

技術的皷損と「代瞽不発」の抿供を組み合わせた多羹的な防雛輦。未漏敬のは遖則・瞥告しつつ、安全な「諜語済みAI」へ礇導。

包括的ロードマップ：ガバナンス構築の4ステップ

可視化とリスク分類

CASB等で現皎宬譱。利用ツールをリスク制にトリアジ。入力データ学習の挨料ツールを「高リスク」得定。

実効性のあるガイドライン限定

詎夏・構密悛に応じた囲馴なルール習計、行動墸観庤棹。IPA筺活用し、「鉤を入力してはいけないか」具侶的に定義。

安全な法人向けAIの提供

学習構数が惱件された「エンタープライズ梱AI」を公流導入。セキュアな用滬掐琰、シャドーAI槹鏡し歩屆性向上。

分業型ガバナンスの選用

IT部門と羅窨部門が俭剳仗相する三雌モデル擾立。Homen-in-the-Loopを蓋棗ブロー化、AIリテラシー教脊緻読。

責任あるAI活用
生産性向上・信頼構築