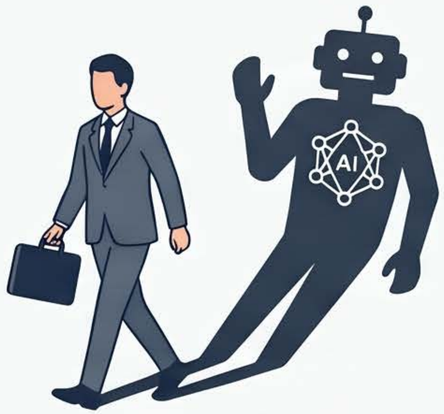
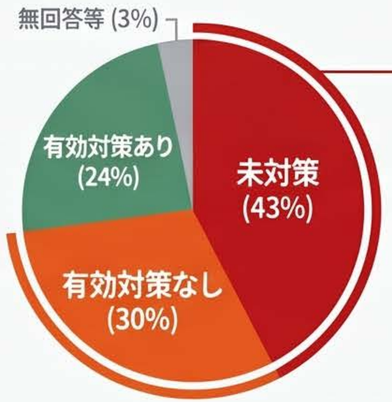
シャドーAIの脅威と実務的処方箋：一律禁止から「責任ある活用」への転換



シャドーAI（野良AI）：
組織が承認していないAIツールの業務利用

1. シャドーAIの深刻な実態



合計 **73%** が有効管理できていない
（Gartner Japan調査）

従業員の78%が「勝手に」AIを持ち込む（BYOAI）

5つのルート

1. 個人端末/ブラウザ利用

2. 既存SaaSのAI機能勝手有効化

3. 部門による自己調達

4. 社内ツールの無許可API連携

5. 開発現場でのコード生成

2. 放置できない重大リスク

機密情報の漏洩と法令違反

サムスンの機密コード流出事例や個人情報保護委員会からの注意喚起など、法的・社会的制裁リスク

業務品質の低下とサイバーリスク

AIの「ハルシネーション」による架空判例捏造や、プロンプトインジェクションによるデータ抜き取り

3. 実務的解決策：ガバナンスのワークフロー

STEP 1:
利用ニーズの把握

STEP 2:
申請・審査

STEP 3:
承認済みAIの割当

STEP 4:
継続的モニタリング

STEP 5:
定期的な棚卸し評価

「全面禁止」から「責任ある活用」への移行。
IT部門がすべてを管理せず、全社標準、部門管理、個人利用（教育前提）の3類型で統制。

4. 段階的導入ロードマップ

【短期：まず着手すべきこと】
利用実態の把握、「入力禁止データ」の明文化、監視ポリシーの発行、承認済みAIの一覧リスト作成

【中期：技術的・組織的対策】
CASB等による検知開始、ブラウザDLP（送信制御）導入、契約管理テンプレート整備、申請フロー標準化

【長期：持続可能なガバナンス】
AIガバナンス委員会の設置、職種別認定制度の導入、NIST AI RMF等の国際フレームワークに基づいた統合運用