bloom株式会社｜AIX事業部

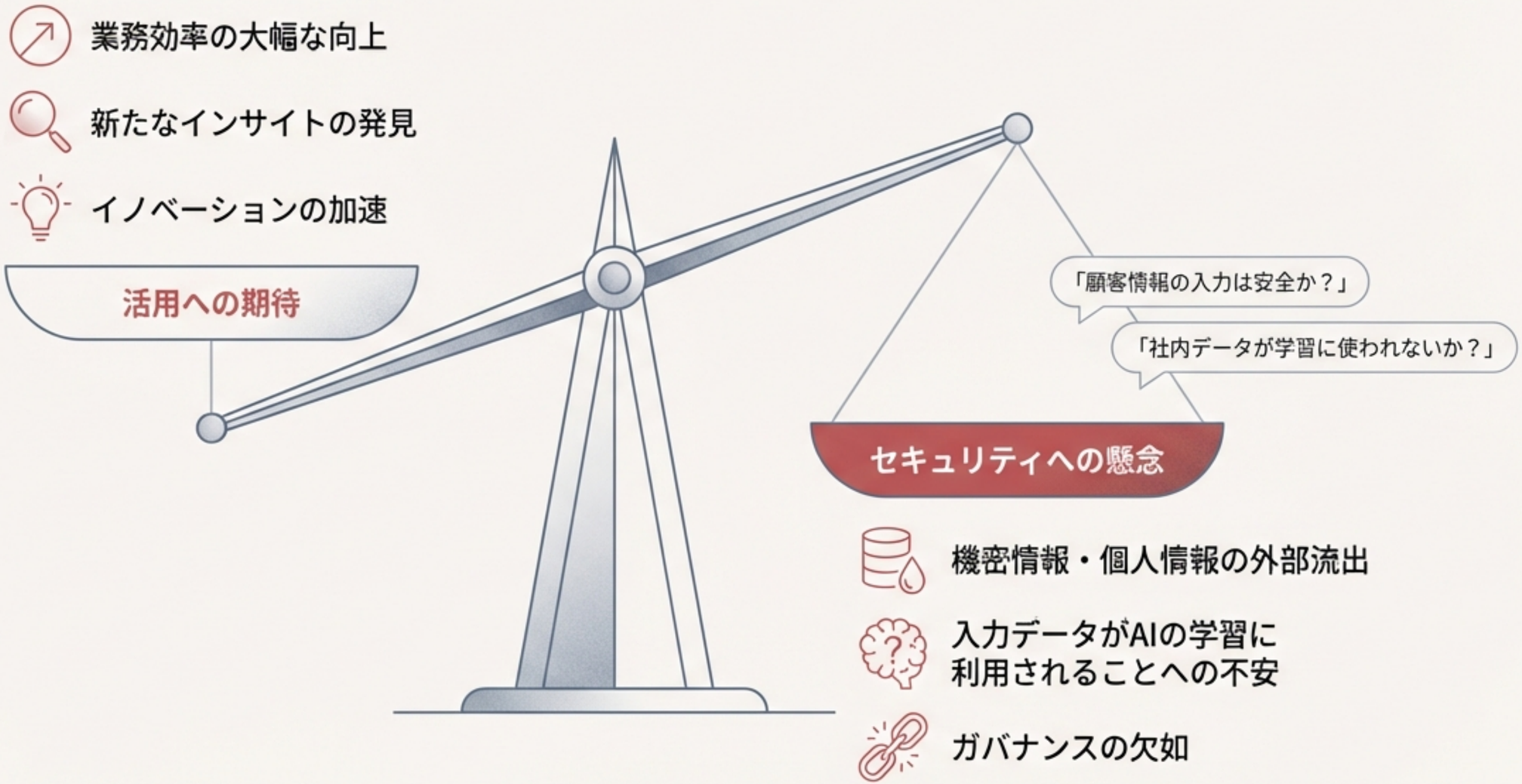
セキュリティと活用推進を両立する、AI業務環境の「設計思想」

「情報漏洩が怖い、でもAIは使わせたい」――
この普遍的ジレマを乗り越えるための実践的フレームワーク

NotebookLM

すべての企業が直面する「AIセキュリティのジレンマ」

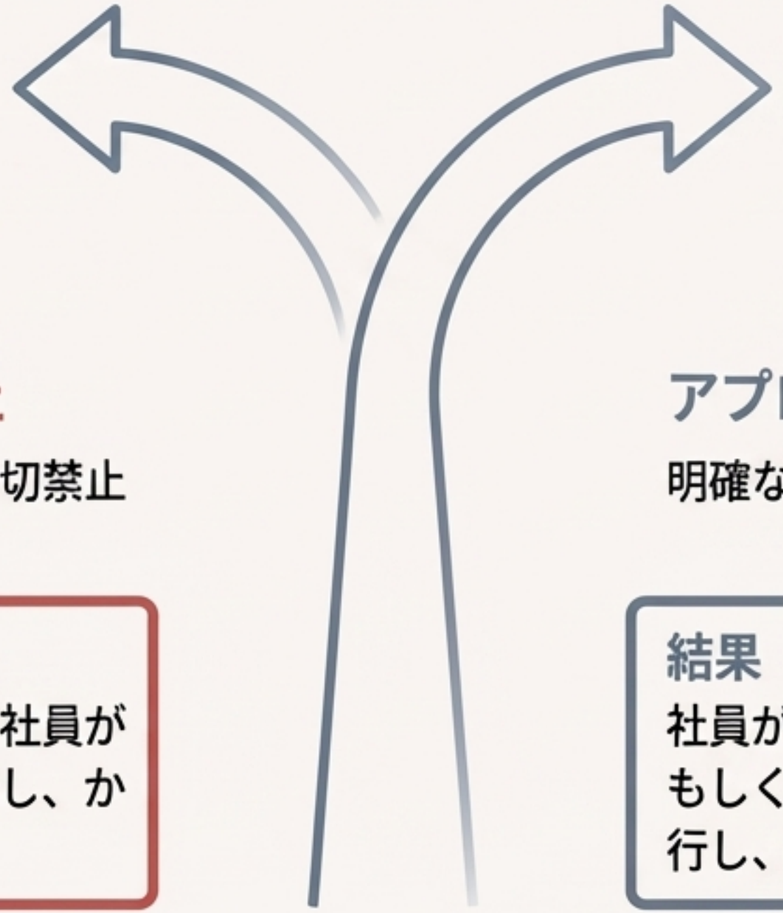
AIの可能性は大きい。しかし、情報漏洩のリスクが活用推進の最大の足かせとなっている。



NotebookLM

ジレンマへの典型的な、しかし機能不全に陥る2つの対応







アプローチ1: 全面的な利用禁止

リスクを恐れ、生成AIツールの利用を一切禁止する。

結果

業務効率化の機会を損失。シャドーIT（社員が個人でAIを利用する「野良AI」）を誘発し、かえってリスクが増大する。

アプローチ2: 曖昧なルールでの運用

明確な方針を定めず、現場の判断に委ねる。

結果

社員が不安を感じてAI利用に消極的になる。もしくは、セキュリティ意識の低い利用が横行し、インシデントのリスクが高まる。

NotebookLM

発想の転換：「禁止」から「環境設計」へ

**セキュリティをAI活用の「制約」と捉えるのではなく、
安全な活用を促進する「土台」として設計する。**

旧来の発想（Old Paradigm）



リスクを回避するために機能を制限する。
セキュリティ部門が「番人」として振る舞う。

我々の選択（Our Paradigm）



社員が安心して使える公式環境を整備する。
「野良AI」を使いたくなる動機そのものをなくす。
セキュリティはイノベーションを加速させるための
基盤である。

NotebookLM

解決策：bloomが実践する「2層構造」のAI業務環境



Layer 2: 専門組織レイヤー（Expert Organization Layer）

対象： AIX事業部（AIリテラシーが高い専門家）
目的： 攻めのAI活用、先進的な活用法の開拓
ツール: Claude, ChatGPT（上位プラン）



Layer 1 : 全社レイヤー（All-Company Layer）

対象： 全社員
目的： 誰でも安全に使えるAI活用の基盤
ツール: Gemini for Google Workspace

社員のリテラシーとセキュリティ要件に応じてツールを分離・最適化することで、活用推進とガバナンスを両立させる。

NotebookLM

【全社レイヤー】基盤となるのは「業務に溶け込むAI」

導入ツール：Gemini for Google Workspace （企業向け有料版）

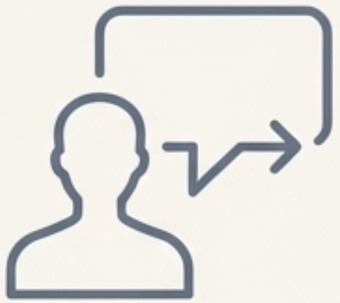
選定理由

- **1. 圧倒的な近接性**
  - Gmail、ドキュメント、スプレッドシートなど、日常業務で使うツールに標準で組み込まれている。
  - 特別なツールを新たに起動する必要がなく、活用のハードルが極めて低い。
- **2. 学習コストの低さ**
  - ITリテラシーに関わらず、普段の業務の延長長線上でAIを使い始められる。
- **3. 業務基盤の統一**
  - 情報がGoogle Workspace内に集約され、AI活用の土台となるデータ基盤が整う。



NotebookLM

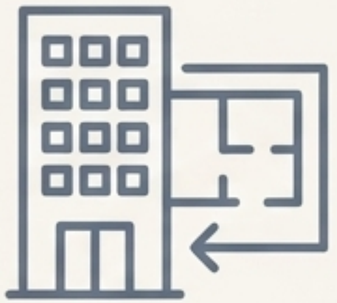
現場での活用シーン：Geminiが日常業務をどう変えるか



キャリアアドバイザー業務

「候補者の強みを3つのポイントで整理して」

- **スカウトメール作成支援**
  候補者に合わせた文面を数秒で生成。
- **面談準備の壁打ち**
  候補者の経歴を基に、「強みをどう整理すべきか」「転職理由の伝え方」などをGeminiと相談し、カウンセリングの質を向上。
- **求人企業の調査**
  企業の特色や求める人物像を瞬時に要約。



不動産領域

- **物件パースの作成**
  従来は外部委託や専門担当者が必要だった作業を、テキスト指示で内製化し、効率を大幅に改善。

NotebookLM

全社展開を可能にする、エンタープライズグレードのセキュリティ

入力データは学習に利用されない

Googleが公式ドキュメントで明文化。機密情報や個人情報を含む業務データも安心して入力可能。

「野良AI」利用リスクの低減

公式に安全なツールが提供されることで、社員がリスクの高い無料AIサービスを個人的に利用する動機を抑制。



人間によるレビューの不在

入力内容をGoogleの従業員が閲覧することはない。

注記：

注記：個人向け無料版Geminiは学習に利用される可能性があり、業務利用は禁止。企業向けプランが必須。

NotebookLM

【専門組織レイヤー】

AIX事業部による「攻めのAI活用」



目的

全社のAI活用レベルを牽引する先進的な活用法を開拓し、その知見を全社に還元する。

役割

- 最新AIモデルの性能検証と業務適用実験
- 全社向け活用ガイドラインの策定
- 各部門へのAI活用コンサルティング

付与ツールとコスト

ツール

Claude（チームプラン）

ChatGPT（チームプラン）

コスト

1人あたり月額3万円〜4万円程度

理由

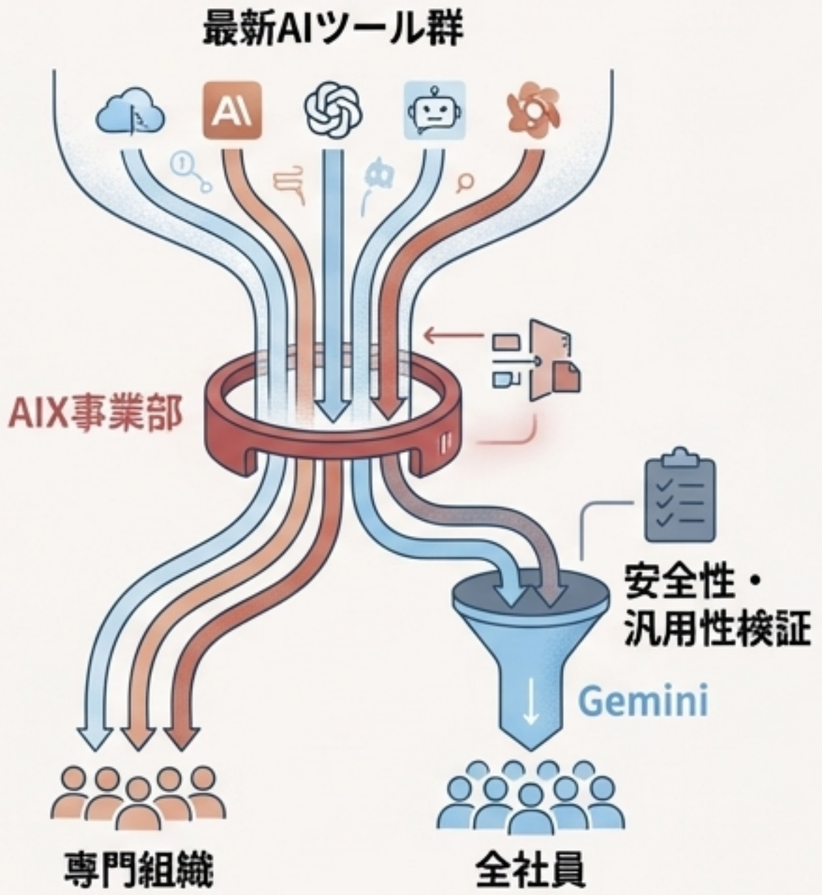
それぞれに異なる強みがあり、用途に応じた使い分けで成果を最大化する。

NotebookLM

なぜ高機能ツールを「限定付与」するのか？

● リテラシーとリスクのバランス

高機能ツールは強力だが、使いこなすには相応の知識が必要。誤った利用はセキュリティリスクを高める可能性がある。



● コスト効率の最大化

全社員に高コストなツールを配布するのではなく、投資対効果が最も高い専門組織に集中投下。

● 「守り」と「攻め」の両立

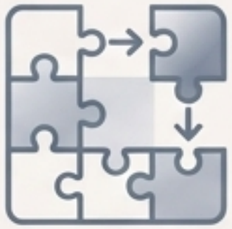
AIX事業部が「攻め」の活用でトップラインを上げつつ、
「全社展開しても安全な活用法」と「専門組織に留めるべき活用法」を見極める役割を担う。

NotebookLM

実践的な導入ロードマップ：我々はこの順番で構築した

STEP 1 → STEP 2 → STEP 3







STEP 1: 専門組織の先行立ち上げ

全社展開の旗振り役として「AIX事業部」を設立。

先行して知見を蓄積。「何が使えて、何が危険か」を把握し、全社展開時のリスクを大幅に軽減。

STEP 2: 業務基盤の統一

AIX事業部を主軸に、全社の業務環境をGoogle Workspaceへ移行。

Geminiを全社で活用できる土台を整備。AIX事業部で先行運用し、課題を洗い出してから他部門へ展開。

STEP 3: 全社への浸透と活用促進

各部門への説明会、業務に即した活用事例の共有、サポート体制の整備。

ツールを「導入する」だけでなく「実際に使われる」状態を創出。

いきなり全社展開せず、専門組織での検証から始めるアプローチがリスク管理の鍵。

NotebookLM

AI環境を支える、徹底したセキュリティ基盤

AIツール自体の安全性だけでなく、アクセス経路の保護が極めて重要。



「野良AI」を不要にする環境

公式ツールをいつでも使える状態にすることで、外部サービスを探す必要性をなくす。



厳格なアカウント管理

全アカウントに2段階認証（2FA）を必須設定。アカウント乗っ取りによる情報漏洩を防止。



徹底した端末管理

Google Workspaceの管理機能を活用し、承認された端末からのみアクセスを許可。私用端末からのアクセスも、セキュリティ要件を満たした場合に限定。

NotebookLM

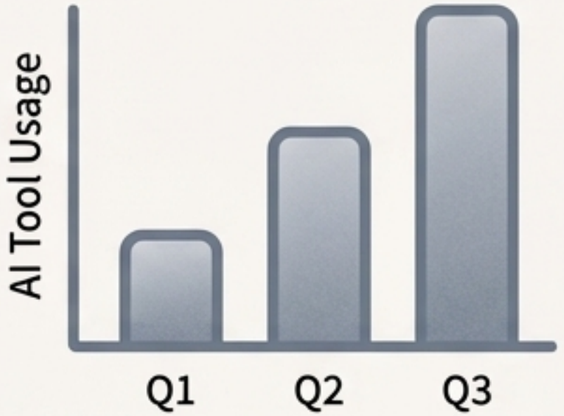
2層構造がもたらした成果

マネージドなAI環境の構築により、セキュリティとイノベーションの両立を実現。



情報漏洩リスクの低減

「野良AI」の利用を抑制し、ガバナンスの効いた環境を確立。



全社的なAI活用の実現

ITリテラシーを問わず、全社員が安全な環境でAIの恩恵を享受。



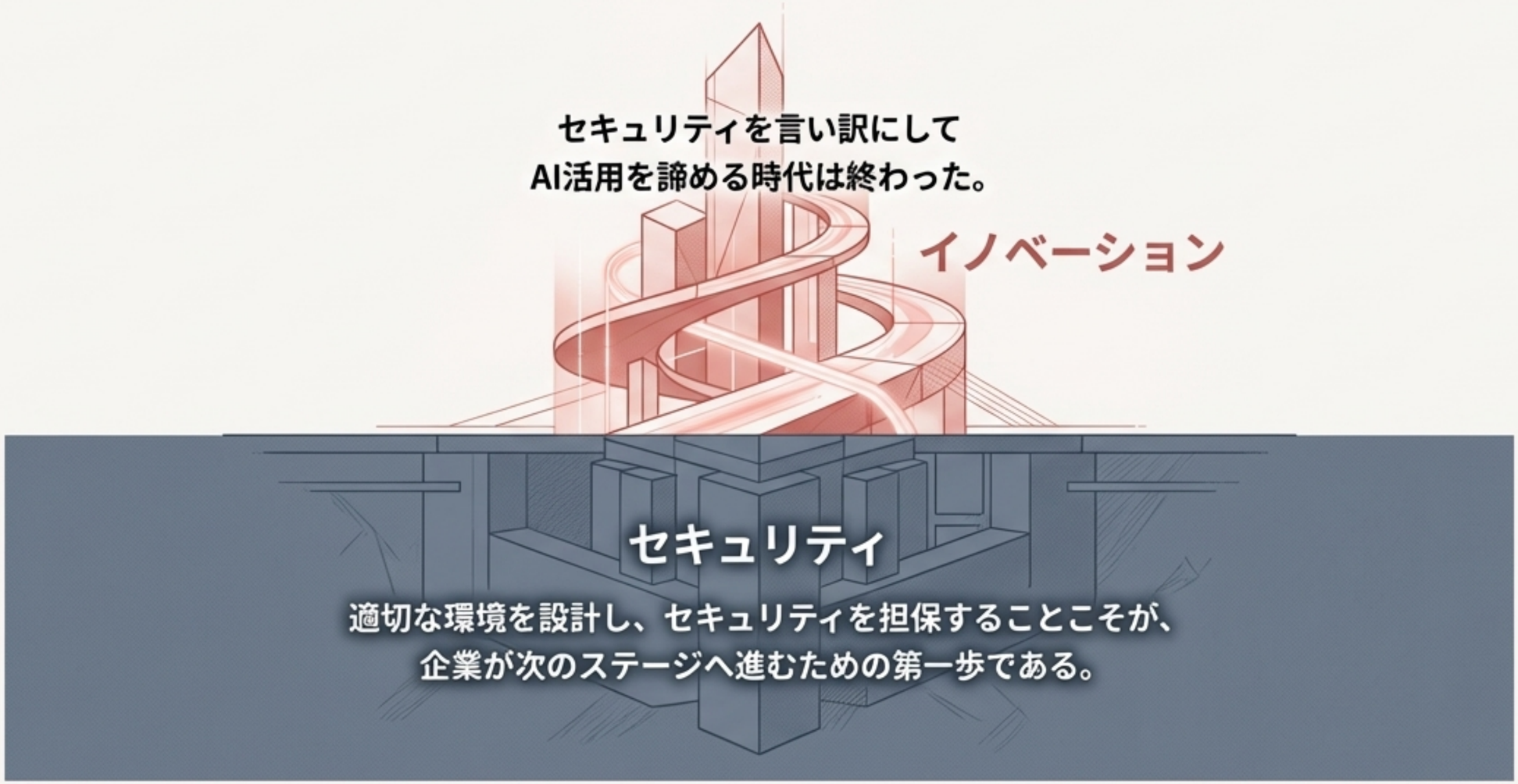
経営層の安心

リスクマネジメントの基盤が整い、経営層が安心してAI活用推進の意思決定を行える状態に。

「リスクを管理下に置くことで、初めて自信を持ってアクセルを踏み込める」

NotebookLM

セキュリティを「制約」から「イノベーションの土台」へ



あなたの会社では、セキュリティは「ブレーキ」になっていますか？
それとも、安心して攻めるための「強固な土台」になっていますか？

NotebookLM