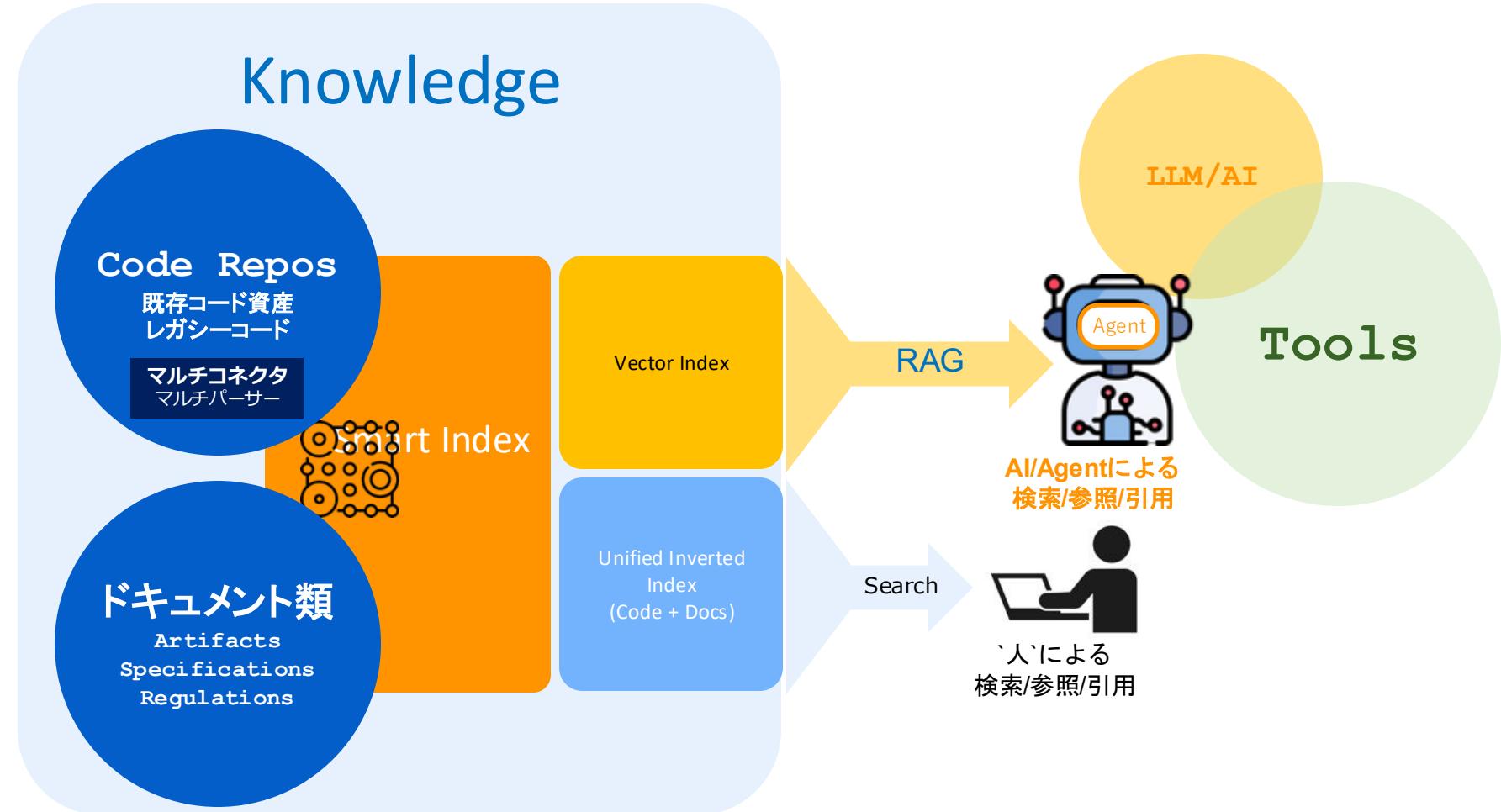




Krugleが提供する
'Knowledge'

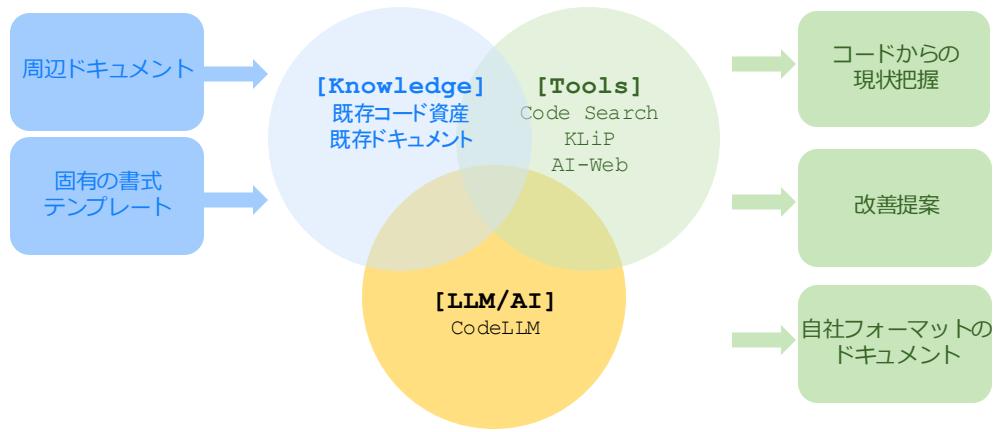


活用事例

ユースケース①:

現状のコードベースのアセスメント

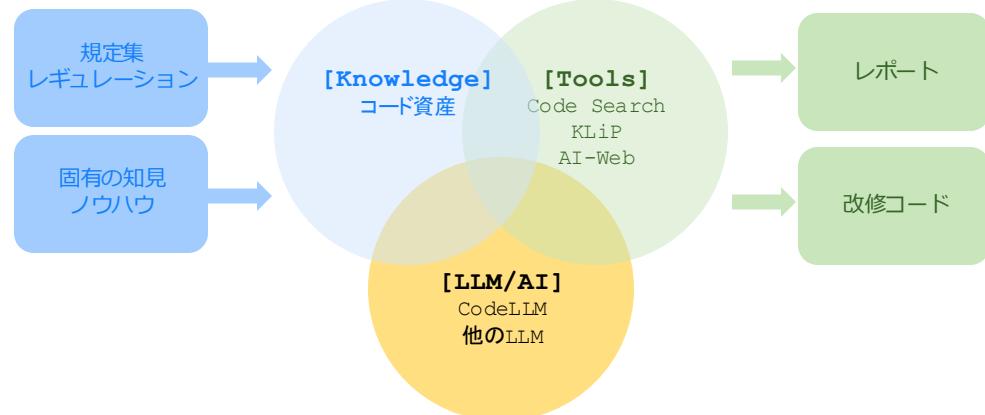
- ✓ 現状課題の把握
- ✓ ドキュメントのアップデート



ユースケース②:

整合性/準拠性の確認及び改修

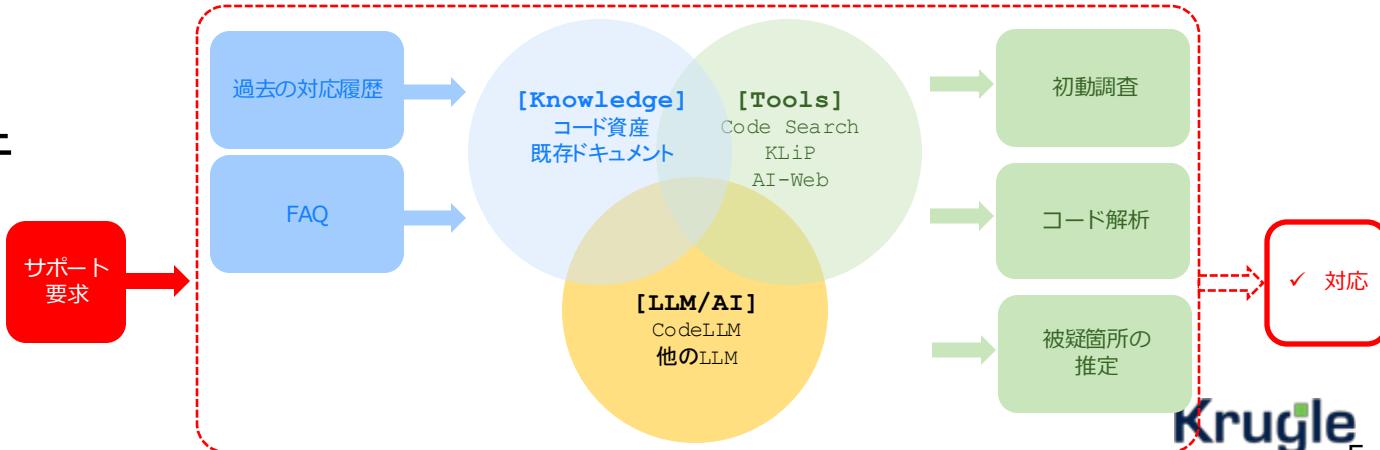
- ✓ vs. 既存ドキュメント
- ✓ vs. ルール/ポリシー
- ✓ vs. 規定/レギュレーション



ユースケース③:

システムサポートの品質効率の向上

- ✓ 対応工数の削減/所要時間の短縮
- ✓ スキルの補完



生成AIを取り巻く構造変化と新たな潮流

顕在化するセキュリティの懸念

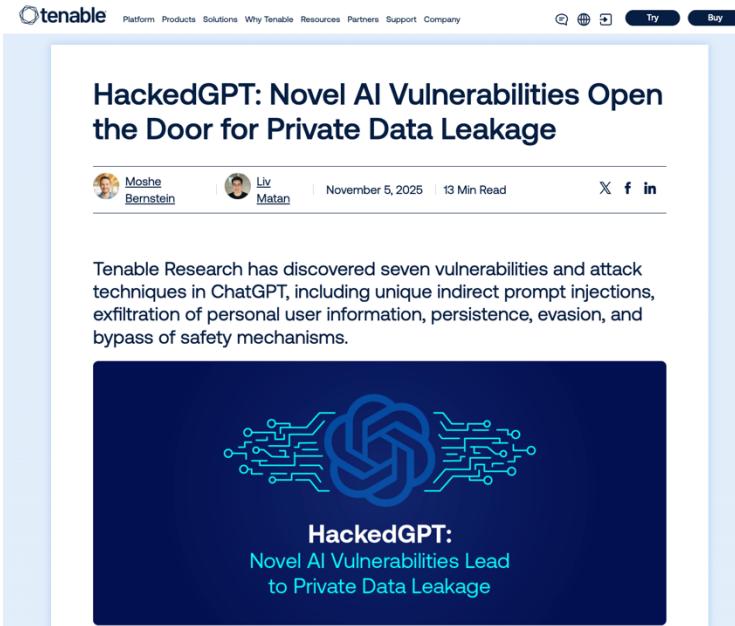
2025年11月5日

HackedGPT：新たなAIの脆弱性が個人情報漏洩の扉を開く

Tenable Research は、ChatGPT に、独自の間接プロンプトインジェクション、個人情報の流出、永続性、回避、安全メカニズムのバイパスなど、7つの脆弱性と攻撃手法を発見しました。



出典：[Tenable - HackedGPT Report 2025.11.05](#)

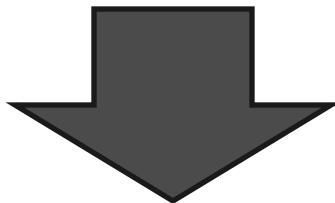
A screenshot of a blog post titled "HackedGPT: Novel AI Vulnerabilities Open the Door for Private Data Leakage" from the Tenable website. The post is authored by Moshe Bernstein and Liv Matan, dated November 5, 2025, with a 13-minute read time. The content discusses seven vulnerabilities in ChatGPT, including unique indirect prompt injections, exfiltration of personal user information, persistence, evasion, and bypass of safety mechanisms. A dark blue sidebar on the right features the "HackedGPT" logo and the text "HackedGPT: Novel AI Vulnerabilities Lead to Private Data Leakage".

重要なポイント：

1. Tenable Research は、OpenAI の ChatGPT に複数の新しい永続的な脆弱性を発見しました。これにより、攻撃者がユーザーの記憶やチャット履歴から個人情報を盗み出す可能性があります。
2. 最新の GPT-5 モデルに存在するこれらの脆弱性により、攻撃者は、ChatGPT に質問するだけを含む、被害者になり得るいくつかの使用例を通じて、ユーザーに知られずにユーザーを悪用する可能性があります。
3. 発見された脆弱性には、ユーザーをこのような攻撃から保護するための ChatGPT の安全機能を回避する脆弱性が含まれており、これにより ChatGPT ユーザーのプライバート データが盗まれる可能性があります。
4. 何億人のユーザーが毎日 LLM とやり取りしており、これらの攻撃に対して脆弱である可能性があります。

根強く残る「Excel仕様書」が妨げる「AIの可読性」

- ✓ 日本では、詳細設計書などのドキュメントはExcelで書かれるケースが大多数
- ✓ 一方、海外ではドキュメント管理/コラボレーションツールへの移行が進んでいる
欧米： Jira + Confluence、Notion、Azure DevOpsに代表されるツールの活用が主流
アジア圏： 旧来のExcel/Word中心の運用からConfluenceやFeishu(中国)などへの移行が加速



Excelドキュメント = AIモデルでは読めない情報資産

LLM → RAG → Agentic RAGへ

Agentic RAGによる自立型回答精度担保

AI活用でユーザーに求められる高いスキルの補完にAIを活用

Agentic RAGに必要なコンポーネントのパッケージング

ユーザーが求める用途に応じたプリフィックス型アプリの提供

ExcelやPDFなどのドキュメントを解析

ユーザーが求める用途に応じたプリフィックス型アプリの提供

Krugle

将来に向けた展望と
製品進化のロードマップ

Agentic RAG

エンタープライズ用途の
Agentic RAGプラットフォームとして
必要なコンポーネントを網羅的にパッケージング

