

Frontline Report

“攻め”のAIに“堅牢な守り”を！OWASP フレームワークで築く LLM セキュリティ

生成AIの業務適用が広がる中、その基盤となる大規模言語モデル(LLM)特有のセキュリティリスクが、企業にとって新たな懸念材料となっている。こうした動きを受け、世界最大級のセキュリティ・コミュニティであるOWASP(Open Worldwide Application Security Project)が2024年に公開したのが「OWASP Top 10 for LLM」だ。世界中の500名以上の専門家による知見をもとに、不適切

な出力の誘導や情報漏洩、過負荷を狙った攻撃など、生成AIに固有のリスク項目を体系的に整理したものである。

このフレームワークを受けて、AIシステムの開発・運用でも“守り”の観点が一段と重視されるようになった。生成AIのポテンシャルを最大化するには、“攻め”の活用と同時に、“守り”の設計が不可欠だ。今後のAI活用には、技術的な革新と倫理的・安全な実装の両立が求められる。

Rank	リスク項目	典型シナリオ
1	Prompt Injection	利用者が巧みな指示を入力し、機密情報を引き出したり別の命令を実行させたりする。
2	Insecure Output Handling	モデルが出力した HTML やスクリプトに XSS などの攻撃コードが含まれ、閲覧者のブラウザで実行される。
3	Training Data Poisoning	公開フォーラムなどから収集したデータに偽情報を混入され、モデルが誤った結論を出すよう誘導される。
4	Model DoS	ボットが大量に問い合わせを送り、推論サーバーが遅延・停止。サービス全体が使えなくなる。
5	Supply-Chain Vulnerabilities	外部モデルやライブラリの更新でマルウェアが混入し、本番環境に侵入される。
6	Sensitive Information Disclosure	社内文書を学習させたモデルが、質問に対して契約書や個人情報をそのまま返してしまう。
7	Insecure Plugin Design	LLM から呼び出す外部ツールが認可チェックを持たず、勝手にファイル削除や送信が行われる。
8	Excessive Agency	モデルに“自動実行”権限を広く与えた結果、意図しないデータ更新やメール送信が発生。
9	Overreliance	生成された内容を検証せず業務に流用し、誤情報がレポート・契約書に反映される。
10	Model Theft	重みファイルが流出し、競合にコピーされる。知財・コスト優位が失われる。

CTC、Google Cloud Next Tokyo' 25に出展

8月5～6日に東京ビッグサイトで「Google Cloud Next Tokyo' 25」が開催される。金融を含めた様々な業種での生成AI活用事例を中心に、RAG構成、MCP対応、BigQuery連携などの最新ソリューションが紹介される。CTCもAI活用に関する展示ブースを出展見込み。生成AI時代のクラウド戦略を牽引する場として要注目だ。

FDUA・生成AIガイドラインがVer1.1に改訂、CTCがイベントで登壇・解説

7月14日開催の「金融生成AIガイドライン(第1.1版)リリースイベント」(主催:金融データ活用推進協会/FDUA)で、当社AIエンジニアの福永 圭佑が本ガイドラインの執筆メンバとして登壇。AIエージェントやAIガバナンス等の業界トレンドや、金融実務の現場からのフィードバックを踏まえた改訂ポイントを解説する。

営業チームで加速するAI活用最前線！ 情報共有と提案強化のリアルストーリー

営業現場でも、生成AIの活用が着実に広がっている。特に、情報の集約や提案資料の質向上といった「実務」領域で、日々の業務に自然と溶け込むかたちでAIを取り入れているチームが増加中だ。

金融営業第3部では、情報共有の場として活用してきたNotionに、2024年からAI機能を本格導入。各担当者が記録した商談メモや提案の要点を、AIが自動で要約・分類し、横断的に検索可能な「ナレッジベース」へと昇華させている。これにより、新人でもベテランの知見に素早くアクセスでき、類似業界や課題を持つ顧客に対して即座に有効な提案事例を見出せるようになった。

こうしたナレッジの蓄積と活用が進む中、週報のスタイルも変化している。以前はExcelで提出していたため、他のメンバーの進捗をリアルタイムで把握することが難しく、会議での情報共有にもズレが生じていたという。しかし今では、Notionに記載した週報をAIが自動要約し、打ち合わせの場でも自然と「XXさんの案件は今こうだね」と話題に上がるように。週報が“提出物”から“会話の入口”に変わり、議論のテンポやチームの一体感も格段に向上した。



さらに、提案資料の作成でもAIが力を発揮している。ヒアリングメモから構成を整理したり、過去の資料をもとに構成案を生成したりすることで、資料作成のスピードと質の標準化を同時に実現。見落としがちな顧客ニーズをAIが補完する場面もあり、「人とAIの協働」が実感できる業務が増えてきた。

「AIがすべてを代替するわけではなく、あくまでサポート役。うまく使えば、チームの底上げにつながる」と担当者は語る。導入のハードルを上げすぎず、日常のツールに組み込むように使う姿勢が、現場での定着を支えている。

最近では、商談の振り返りや顧客の反応の要点整理など、さらなる応用も進行中だ。これらの積み重ねが、提案のスピード感と社内連携の円滑化を後押ししており、「AI×営業」は単なる業務効率化にとどまらず、提案の質を高める起点となりつつある。

生成AIの活用は、今後もより多様なかたちで進化していくだろう。その進化を形にしていくのは、最前線の現場だ。現場こそが、AIを“使いこなす力”を育み、未来の営業のあり方を更新していく。



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group



CTC金融事業グループの最新情報は
オウンドメディアサイトへ！

<https://financial.ctc-g.co.jp/>



お問い合わせ

CTC
Challenging Tomorrow's Changes

伊藤忠テクノソリューションズ
金融事業グループ金融NEXT企画部

✉ fsgnext-biz-dev@ctc-g.co.jp