

応募課題（AIレッドチーミング・クラス）

【問 1】

攻撃者の気持ちで以下の問に答えてください。

チャットボットやコード補完・自動生成、ドキュメント作成支援など、LLM（大規模言語モデル）を活用したアプリケーション（以下、LLMアプリケーション）が増えています。

このようなLLMアプリケーションは、LLM単体の能力を活用するだけではなく、データベースやWeb APIなどの外部システムと連携することで、より柔軟な処理を行うことができます。

LLMアプリケーションと【連携する外部システム】を攻撃（情報窃取やデータ改ざん、削除など）する場合、どのような攻撃シナリオを構築しますか。具体的に回答してください。

なお、攻撃者はLLMアプリケーションに入力する「プロンプト」を細工できますが、直接外部システムにアクセスできないものとします。

応募課題（AIレッドチーミング・クラス）

【問2】

システム運用者の気持ちで以下の問に教えてください。

【問1】の攻撃に対し、あなたはどのような対策を採用しますか。

対策の実効性（技術的難易度、対策の運用コスト、アプリケーションのUXなど）を考慮し、現実的な対策を立案してください。