応募課題

この選考課題は、知識の正誤を判断するだけのものではなく、あなたの経験や興味関心の幅や深さ、物事への取り組み方を問うものです。

よって原則として、一般的な"学力テスト"とは異なり、自由に調べたり、実験したり、ChatGPTやGeminiなどのLLMサービスを活用していただいて構いません。

ただし、個別の課題において指定がある場合は、その指定に従ってください。

様々なものを活用し、自分で理解して意見をまとめ、納得できる回答を仕上げて提出してください。

- 【問1】は必須問題です。問題は４問ありますが、４問中２問以上回答してください。
- ２問以上回答した場合はすべて採点し、点数の高い２問の得点を元に判断いたします。

応募課題

【 問１】共通

あなたがミニキャンプに応募された動機について教えてください。また、この講義で学んだことを何に役立てたいかを教えてください。

【 問２-１】

普段使っている、または今後使ってみたいと思っているLLMアプリ（例：ChatGPT、Cursorなど）を一つ挙げて、そのアプリがどのように動いているか、自分なりに説明してみてください。

応募課題

【 問２-２】

そのアプリで、もし何か良くないことや困ったことが起こるとしたら、どんなことが考えられるか、想像して書いてみてください。（例：うっかり個人情報を入力してしまい、それが他の人に見られてしまう／AIが間違った情報をそれっぽく答えてくる　など）

【 問３－１】

これまでRustを用いたコーディングの経験がもしありましたら、お教えください。

ない場合は、それ以外で何らかのコーディングの経験がある場合は自由にお書きください。

応募課題

【 問３‐２】

どのようなインターネット技術に興味がございますか？また、自作してみたいものはございますか？

【 問４‐１】

PE ファイルの構造について調べて、おもしろいと思ったものを報告してください。

【 問４‐２】

マルウェアによってよく利用されるテクニックを調べ、報告してください。

応募課題

【 問５－１】

あなたが触ったことがある、または知っている「複数のプログラムやAIが連携して動作する仕組み」にはどのようなものがありますか？それを簡潔に説明した上で、セキュリティ上のリスクを考え、そのリスクに対する対策を簡潔に述べてください。

【 問５－２】

あなたは、LLMベースのAIシステム（チャットボットなど）を使用しているとします。このAIシステムには、あなたが入力したプロンプトを別のAIで解析したり、他のシステム（データベースやコードインタープリターなど）と連携したりする仕組みがあります。このようなAIシステムにおいて、悪意のある利用者が入力するプロンプトを細工することで、AIに意図しない動作をさせたり、AIシステム内部の機密情報を引き出せるとしたら、どのような攻撃シナリオが考えられますか？簡潔に述べてください。