応募課題

これらの選考問題は、あなたの現状の知識や経験、興味関心の範囲や深さ、物事を探求する手法などを問うものです。

一般的な"テスト"とは異なり、自由に調べたり、実験したり、LLMサービスを用いて解いて頂いて構いません。

限られた時間内に答案をまとめること自体が一つの課題であり、講義に必要な知識を埋める作業です。

自分が納得できる回答を仕上げ、提出してもらえれば幸いです。

Bトラック 応募課題（１）

【 問１】

あなたがミニキャンプに応募した動機について教えてください。
また、以下のこともそれぞれ教えてください。

・期待していること（箇条書きで3つ）

・受講後にやってみたいこと（箇条書きで3つ）

・不安な点／苦手だと思う点

Bトラック 応募課題（２）

【 問２ ：セキュリティの考え方】

以下のシナリオを読んで、(1)(2)に回答してください。

シナリオ：あなたはECサイトのセキュリティ担当者です。ある日、「ログインしていないのに、他人の注文履歴が見えた」という問い合わせがありました。調査の結果、URLの `order_id=123` を `order_id=124` に書き換えると、他人の注文が見えてしまうことがわかりました。

(1) この問題を防ぐために、アプリケーション側でどのような対策が必要だと思いますか。あなたの考えを書いてください。（150字程度）

(2) この問題が起きていたことに「気づける」ようにするには、どのようなログを残し、どのように監視すればよいと思いますか。（150字程度）

Bトラック 応募課題（３）

【 問３ ：技術問題】

以下の仕様を満たすスクリプトを作成してください（言語は問いません）。

仕様：
- 入力：テキストファイル（1行に1つのJSON）
- 処理：各行をJSONとして読み込み、`user_id` ごとに出現回数をカウント
- 出力：ユーザーごとのカウントを表示

入力例：
```
{“user_id”:“alice”,“action”:“login”}
{“user_id”:“bob”,“action”:“view”}
{"user_id":"alice","action":"purchase"}
```

出力例：
```
alice: 2
bob: 1
```

Bトラック 応募課題（４）

【 問４ ：調査・考察】

「DNSを使ったデータ持ち出し（DNSトンネリング等）の防御」というテーマについて、
1：持ち出しが成功する理由
2：持ち出しが行われている兆候を3つ以上
3：対策案
4：あなたが担当者だとして、最初の一歩として何を行うべきか（理由付きで）
を記載してください。

なお、対策案は、次の4つの箱に分けて提案してください。
・検知（Detection）：何を見て怪しいと判断するか
・抑止（Prevention）：どう制限・遮断するか（やりすぎ注意も含む）
・運用（Operations）：誤検知や例外が出た時にどう回すか（誰が何をするか）
・副作用（Trade-off）：正当な通信が壊れる可能性／プライバシーへの配慮

ヒント：
・本問は「攻撃手順を詳しく書く」ことが目的ではありません。防御側の理解と設計を目的にしています。
・この講義は「DNSサーバを作る」だけでなく「ログ（可観測性）→分析→運用設計」まで扱います。
・1「持ち出しが成功する理由」は、例えば「DNSがどんな用途の通信か」「ネットワーク的に通りやすい背景」などを考えるとわかりやすいです。
・2「持ち出しが行われている兆候」は、例えば問い合わせ名が長い、特定の種別に偏る、失敗率が高い…などがありますが、あなたの推測でOKです。

Bトラック 応募課題（５）

【 問５ ：ネットワークの流れを説明 】

調査の際は、インターネット検索、YouTube、ChatGPTやGeminiなどの生成AIを積極的に活用してください。
なお、問5-1のみ必須であり、問5-2と問5-3は余裕があれば解答してください。

【問５-１】（必須）

あなたがブラウザで Webページを開くとき、裏側で起きることを説明してください。説明には、以下に示す単語を必ず使用してください（順番は自由です）。可能であれば、送受信されるデータの例（短い例でOK）も書いてください。

使用する単語：

- スタブリゾルバ
- 権威DNSサーバ
- DNSレスポンス
- TTL
- HTTP GETリクエスト
- 再帰リゾルバ（リカーシブリゾルバ）
- DNSクエリ
- Aレコード（またはAAAAレコード）
- TCP 3-way handshake

DNSに詳しくなくても大丈夫です。ポイントは「名前をIPに変える流れ」「その後にHTTP通信が始まる流れ」を、あなたの言葉で筋道立てて説明することです。

Bトラック 応募課題（６）

【 問５-２ ：軽い実験 】<任意>

DNSを“体験”してみてください。以下のどちらでもOKです。
A：自分のPCで nslookup または dig（使える方）を実行し、結果を貼って説明
B：オンラインのDNSチェックツール等で調べ、結果を貼って説明（ツール名も書く）

最低限やってほしいこと：
何か1つドメインを選んで、名前解決の結果を示す（出力貼り付け）
その結果から分かることを3つ書く（例：IPが返ってきた、TTLが見える、CNAMEがある等）
「ログを取るなら、どの情報があると嬉しいか」を3つ書く（理由も）

Bトラック 応募課題（７）

【 問５-３ ：設計問題 】＜任意＞

「DNSのログ（可観測性）」を設計してみてください。
講義で作るDNSサーバを運用すると仮定し、1リクエスト1行のログとして、あなたならどんな項目を残しますか？

必須：最低6項目以上（例：時刻、送信元、問い合わせ名、種別、応答コード、サイズ…など）
追加：「残さない方がよい情報」（プライバシー/安全面）も1つ書く
　　そのログで「怪しさ」を見つけるなら、どんな集計（メトリクス）が欲しいか（2つ以上）

【任意】あなたの工夫
あなたが今回の課題で 使った情報源（Web/動画/書籍/LLM）を列挙し、「どれが役に立ったか」「どう活用したか」を短く書いてください。
LLMを使った人は、差し支えなければ
・どんなプロンプトを投げたか（要点だけ）
・その出力をどう検証/修正したか
を書いてください（丸ごと貼り付けは不要）

参考情報（提出の末尾に記載）
・参考にしたURLや動画タイトル（箇条書きでOK）
・LLMを使った場合：使ったサービス名（ChatGPT / Geminiなど）と用途（要約、言い換え、理解補助など）

Bトラック 応募課題（８）

【 問６ ：自由記述 】＜任意＞

以下のいずれか1つを選択し、回答してください。（300字程度）

選択肢A：
あなたがセキュリティに興味を持ったきっかけと、これまでに取り組んだこと（CTF、学習、開発など）を教えてください。

選択肢B：
「攻撃手法を学ぶこと」は「防御に活かすこと」にどうつながると思いますか。あなたの考えを書いてください。

選択肢C：
AIがサイバーセキュリティの分野でどのように活用できると思いますか。期待することと懸念することを書いてください。