

1) 「悪意あるソフト・攻撃/防御」について用語や考え方を一通り押さえておこう。次の言葉(概念)を2~3行程度で説明せよ

- (1) マルウェア(コンピュータウイルス) ~ どういうもので、何をするか、何が問題か
- (2) スパイウェア
- (3) フィッシング
- (4) キー・ロガー
- (5) DoS 攻撃、DDoS 攻撃
- (6) アンチウイルスソフトウェア(ワクチン)
- (7) ファイヤウォール
- (8) パケット・フィルタ
- (9) ソーシャルエンジニアリング
- (10) IDS (Intrusion Detection System、侵入検知システム) 教科書には無いが、自分で調べてみよ

2) 攻撃と防御について、できる範囲で整理してみよう。

- (1) ユーザのデータが、意図に反して読まれたり書き換えられたりすることを防ぐ(OS の)仕組みは、どうなっているか?
  - \* 第三者によるデータの読み書きを防ぐ
  - \* 第三者によるプログラムの実行(によって読み書きする・読み書きできるように許可を変更する)を防ぐ
  - \* 高権限コード(高権限を持つユーザ(システム管理者など)になります、または OS(カーネル)の内部コードとして実行する)の実行を防ぐ 授業では取り上げなかったが、OS カーネルの保護の仕組みに関わる。自分で調べてみよ。
- (2) 上記(1)を破る方法として、どのようなものがあるのか?
- (3) ユーザのアプリケーションがユーザのデータを書き換えることは、できて当たり前なのだが、思わぬ形で書き換えることによって悪事をはたらく場合がある。たとえば、アプリケーションをうまく騙すことによってデータを不正に書き換えて、データを壊したり詐欺を働いたりする事件が起きる。簡単な例である「SQL インジェクション」と呼ばれる手法について、ネット等で調べてみよ。どういう仕組みのときに、どういう原理で、何をどうすることができるのか? 対応策は何か? OS やネットワークで提供されるセキュリティの仕組み・仕組み(アンチウイルスソフトやファイヤウォール)では防御できないのだが、それはなぜか?
- (4) 上記(1)の DoS 攻撃(DDoS を含む)に対して、OS やネットワークで提供されるセキュリティの仕組み・仕組み(アンチウイルスやファイヤウォール)では防御できないのだが、それはなぜか?
- (5) 上記(1)のソーシャルエンジニアリングを使った攻撃に対して、OS やネットワークで提供されるセキュリティの仕組み・仕組み(アンチウイルスやファイヤウォール)では防御できないのだが、それはなぜか?

今学期の授業のまとめとして、初回に配布した「ルーブリック」に掲載されている例題を再掲する。これらに答えられるようになることが目標であったが、どうだろうか。

- 1) OS とは何をするものか、どういう役に立つのか、無いと何ができないか
- 2) OS の代表的な構造を図示し、各要素の役割を説明せよ。 階層構造のメリットは何か
- 3) 実行管理(CPU 管理・多重処理)に期待する効果は何かを2点説明せよ
- 4) 多重処理の動作を説明せよ。 多重処理がどのような仕組みで実現されるのか説明せよ
- 5) プロセスの概念を説明せよ。 コンテキストの概念を説明せよ
- 6) プロセスの状態の概念と状態遷移について説明せよ
- 7) プロセスのスケジューリングの概念を説明せよ。 バッチとリアルタイムスケジューリングの違いについて説明せよ、
- 8) FCFS・SPTF・ラウンドロビン・EDF について説明せよ
- 9) 並行処理と並列処理の違いを説明せよ。 同期の必要性を説明せよ。 ロックと排他の概念を説明せよ。 セマフォを説明せよ。 同期機構の実現法と不可分操作、OS による Wait とビジーウェイトの違いを説明せよ
- 10) デッドロックとは何か、どういう状況で起こるのか説明せよ。 デッドロックへの対策について方法と原理を説明せよ
- 11) 共通バッファによる通信・メッセージによる通信の違いを説明せよ。 セマフォによる共通バッファの実現法を説明せよ
- 12) デバイスの管理の必要性を説明せよ。 デバイスの排他管理を説明せよ。 デバイスの仮想化を説明せよ
- 13) バッファリングの原理と効果を説明せよ。 ブロッキングの原理と効果を説明せよ。 スプーリングの原理と効果を説明せよ
- 14) ディスクのスケジューリングの原理と効果を説明せよ
- 15) 領域管理とは何か、なぜ必要かを説明せよ
- 16) (外部)フラグメンテーションの発生過程と問題点を説明せよ
- 17) コンパクション・ガベージコレクション(GC)とは何か説明せよ。 コンパクション・GCの問題点を説明せよ
- 18) ベースアドレッシングによる再配置とその問題点を説明せよ
- 19) 大容量に対するオーバーレイによる解決の原理を説明せよ
- 20) ページングの原理とその効果を説明せよ
- 21) デマンドページングの考え方・実装法・効果を説明せよ。 アクセス要求からデータを得られるまでの手順を説明せよ。 ハードとソフトの分担、ページテーブル、ページフォルトを説明せよ
- 22) 参照の局所性とは何か、ヒット率との関係を説明せよ。 ページ置換えアルゴリズム FIFO・LRU について説明せよ。 置換えアルゴリズムによる違い・性能評価法を説明せよ
- 23) 外部記憶スペースのファイル化の効果を説明せよ。 入出力機器の仮想化の考え方・やり方・有用性を説明せよ
- 24) ファイルの名前付けのメリット、トリー型ディレクトリのメリットを説明せよ。 トリー型のパスの記法を例示せよ。 メタ情報とは何か説明せよ。 名前のハッシュによる管理法を説明せよ、
- 25) 領域管理の必要性を説明せよ(特にフラグメンテーション)。
- 26) FAT と UFS の仕組・原理と、利点・欠点を説明せよ。 ログ構造システム・ジャーナリングシステムの原理と利点を説明せよ
- 27) ユーザーインターフェースの概念を説明せよ。 CUI・GUI の考え方と利点・欠点を説明せよ
- 28) ウィンドウシステムとは何か説明せよ。 国際化とローカリゼーションとは何か、その利点は何か説明せよ
- 29) 文字コードの考え方を説明せよ。 ASCII やユニコードについて説明せよ。 字種混在の問題を説明せよ
- 30) 入力メソッドの接続法について説明せよ。 かな漢字変換の概要を説明せよ。 他に入力メソッドについて説明せよ
- 31) セキュリティの概念、システム保護の考え方を説明せよ
- 32) 暗号の考え方、秘密鍵・公開鍵暗号の仕組を説明せよ。 情報秘匿・認証・なりすまし・署名の原理を説明せよ
- 34) マルウェアの概念、攻撃の概念を説明せよ。 ウィルス対策・ファイアウォールについて説明せよ。 ソーシャルエンジニアリング・DDoS 攻撃について説明せよ