IT パスポート試験合格講座 Technology 11

- 情報セキュリティ

1. 情報セキュリティの 3 要素
   (1) 機密性(Confidentiality)
   許可された正規のユーザだけがアクセスできる状態を確保すること。
   (2) 完全性(Integrity)
   情報が正確であり、改ざんされたり破壊されたりしていないこと。
   (3) 可用性(Availability)
   認められた利用者が、必要なときに利用できること。

2. 情報セキュリティポリシ
   企業や組織の情報セキュリティに関する取組みを包括的に規定した文書。情報セキュリティ基本方針、情報セキュリティ対策基準で構成され、組織のトップによって承認されて公表される。

3. ISMS(Information Security Management System)／ISO/IEC 27001 (JIS Q 27001)
   情報セキュリティマネジメントシステムの管理・運用に関する仕組み。保護すべき情報資産を特定し、リスク対策を決める。

4. ISMS におけるセキュリティリスクへの 4 つの対応
   ①リスク移転、②リスク回避、③リスク受容、④リスク低減。

5. リスクマネジメント(Risk Management)
   リスクについて、組織を指揮統制するための調整されたプロセス。一般的に、(1)リスクの特定→(2)リスクの大きさの算定→(3)リスクの大きさの評価→(4)対策の導入の手順になる。

6. リスクアセスメント(Risk Assessment)
   リスク特定、リスク分析、リスク評価までの全てのプロセス。守るべき対象である情報資産で発生する可能性のある脅威と、脅威の発生確率や発生した場合の影響度等を評価する方法のこと。

7. セキュリティホール
   不正アクセスなどに利用される、コンピュータシステムやネットワークに存在する弱点や欠陥。

8. マルウェア（Malware）
   コンピュータウイルス、ワームなどを含む悪意のあるソフトウェアの総称。

9. スパイウェア
   本人に気付かれないように、操作履歴や個人情報などを収集するソフトウェア。

10. ボット
    ネットワークを介して、他人の PC を自由に操ったり、パスワードなど重要な情報を盗んだりするプログラム。

11. クラッキング（Cracking）
    悪意をもってコンピュータに不正侵入し、データを盗み見たり破壊したりする行為。

12. IP スプーフィング（Spoofing）
    偽の送信元 IP アドレスをもったパケットを送る行為。

13. バッファオーバフロー（Buffer Over Flow）
    プログラムが用意している入力用のデータ領域を超えるサイズのデータを入力することで、想定外の動作をさせる攻撃。

14. バックドア
    侵入を受けたサーバに設けられた、不正侵入を行うための通信経路。

15. キーロガー（Key Logger）
    キーボード入力を記録する仕組みや、この記録を入手する行為。

16. ポートスキャン
    TCP/IP のプロトコルのポート番号を順番に変えながらサーバにアクセスし、侵入口と成り得る脆弱なポートがないかどうかを調べる攻撃。

17. ウォードライビング（War Driving）
無線LANの電波を検知できるPCを持って街中を移動し、不正に利用が可能なアクセスポイントを見つけ出す行為。

18. ソーシャルエンジニアリング
巧妙な話術や盗み見などによって、パスワードなどのセキュリティ上重要な情報を入手したり、システムに侵入しようとしたりする攻撃。

19. ワンクリック詐欺
Web サイトの閲覧や画像のクリックだけで料金を請求する詐欺。

20. トロイの木馬
利用者に有用なソフトウェアと見せかけて、悪意のあるソフトウェアをインストールさせ、利用者のコンピュータに侵入する攻撃手法。

21. マクロウイルス
表計算ソフトなどの操作手順を記録する機能を不正に利用する攻撃。

22. フィッシング
金融機関や有名企業などを装い、電子メールなどを使って利用者を偽のサイトへ誘導し、個人情報などを取得しようとする攻撃手法。

23. DoS 攻撃（Denial of Service）
特定のサーバに大量の接続要求を送り続けて、サーバが他の接続要求を受け付けることを妨害する攻撃。

24. 総当たり攻撃／ブルートフォースアタック（Brute Force Attack）
文字の組合せを順に試すことによって、パスワードを解読しようとする攻撃。

25. 辞書攻撃
辞書に載っている単語を入力してパスワードなどを推測しようとする攻撃手法。

26. ゼロデイ攻撃
ソフトウェアに脆弱性が存在することが判明したとき、そのソフトウェアの修正プログラムがベンダから提供される前に、判明した脆弱性を利用して行われる攻撃。

27. パスワードリスト攻撃
どこかの Web サイトから流出した利用者 ID とパスワードのリストを用いて、他の Web サイトに対してログインを試行する攻撃。

28. 水飲み場型攻撃（Watering Hole Attack）
標的組織の従業員が頻繁にアクセスする Web サイトに攻撃コードを埋め込み、従業員がアクセスしたときだけ不正行為が行われるようにする攻撃手法。

29. ランサムウェア（Ransomware）
感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、元に戻すための代金を利用者に要求するソフトウェア。

30. アドウェア（Adware）
画面上に広告を表示させる機能が付いたソフトウェア。

31. SQL インジェクション
データベースに悪意のある問合せや操作を行う命令文を入力して、データベースのデータを改ざんしたり不正に取得したりする攻撃。

32. キャッシュポイズニング（DNS Cache Poisoning）
DNS（Domain Name System）キャッシュサーバに対して偽の DNS 情報をキャッシュとして登録させることで、利用者を偽の Web サイトに誘導しようとする攻撃手法。

33. クロスサイトスクリプティング（XSS、Cross Site Scripting）
Web サイトの運営者が意図しないスクリプトを含むデータであっても、利用者のブラウザに送ってしまう脆弱性を利用する攻撃。

34. セションハイジャック（Session Hijack）
サーバとクライアント間の正規のセッションに割り込んで、正規のクライアントに成りすますことで、サーバ内のデータを盗み出す行為。