IT パスポート試験合格講座 Technology 12

- 情報セキュリティ対策

1. CSIRT（Computer Security Incident Response Team）
   企業・組織内や政府機関に設置され、コンピュータセキュリティインシデントに関する報告を受け取り、調査し、対応活動を行う組織の総称。

2. CRYPTREC（Cryptography Research and Evaluation Committees、クリプトレック）
   電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

3. プライバシーマーク制度
   JIS Q 15001 に基づき、個人情報について適切な保護措置を講じる体制を整備している事業者などを JIPDEC が評価・認定する制度。

4. ファイアウォール
   インターネットからの不正アクセスを防ぐことを目的として、インターネットと内部ネットワークの間に設置する仕組み。

5. コンテンツフィルタリング
   青少年に有害なサイトなどを携帯電話端末に表示しないようにする仕組み。

6. MAC アドレスフィルタリング
   無線 LAN のセキュリティにおいて、アクセスポイントが接続要求を受け取ったときに、端末固有の情報を基にアクセス制御を行う仕組み。

7. アンチパスバック方式
   ID の状態を記録し、入室済みの ID での再入室、退室済みの ID での再退室を規制するセキュリティ対策。

8. VPN（Virtual Private Network）
   インターネットなどの共用のネットワークに接続された端末同士を、暗号化や認証によってセキュリティを確保して、あたかも専用線で結んだように利用できる技術。

9. DMZ（DeMilitarized Zone）
企業内ネットワークからも、外部ネットワークからも論理的に隔離された領域。外部からの不正アクセスによる被害が及ばないようにするためのエリア。

10. SSL（Secure Socket Layer）／TLS（Transport Layer Security）
HTTP 通信の暗号化を行うことによって、通信経路上での通信内容の漏えいを防ぐセキュアプロトコル。

11. HTTPS(HTTP over SSL/TLS)
サーバとブラウザが安全に通信をするために SSL を使って通信内容を暗号化するためのプロトコル。

12. ディジタルフォレンジックス
不正アクセスなどコンピュータに関する犯罪の法的な証拠性を確保できるように、原因究明に必要な情報の保全、収集、分析をすること。

13. ペネトレーションテスト
システムに対して、実際に攻撃して侵入を試みることで、セキュリティ上の弱点を発見しようとする侵入テスト。

14. ワンタイムパスワード
認証のために一度しか使えないパスワード。利用者は、トークンと呼ばれる装置などを用いて生成された使い捨てのパスワードを使って認証を受ける。

15. シングルサインオン
一度の認証で、複数のサーバやアプリケーションなどを利用できる仕組み。

16. コールバック
アクセス権をもつ端末であることを確認するために、回線をいったん切り、システム側から再発信して通信を開始する方法。

17. CAPTCHA
人間には読み取ることが可能でも、プログラムでは読み取ることが難しいという差異を利用して、ゆがめたり一部を隠したりした画像から文字を判読させ入力させることで、人間以外による自動入力を排除する技術。

18. 生体認証／バイオメトリクス認証
指紋や声紋など、身体的な特徴を利用して本人認証を行う仕組み。認証用の ID やパスワードを記憶したり、鍵やカード類を携帯したりする必要がない。

19. 静脈パターン認証（Vein Authentication）
生体認証のひとつ。掌や指先の静脈パターンで本人確認を行う認証方式。

20. 虹彩認証（Iris Recognition）
生体認証のひとつ。角膜と水晶体の間にある薄い膜によって本人確認を行う。

21. マトリクス認証
特定の数字や文字の並びではなく、位置についての情報を覚え、認証時には画面に表示された表の中で、自分が覚えている位置に並んでいる数字や文字をパスワードとして入力する方式。

22. ウイルス対策ソフトのパターンマッチング方式
ウイルス定義ファイル（パターンファイル）を用いて、PC に存在するファイルと照合し、一致すればマルウェアとして検出する手法。導入後もウイルス定義ファイルの更新を継続して行う必要がある。

23. 暗号化／復号
暗号化は通信文の内容を秘匿するための変換方法。暗号文を平文に戻すことを復号という。

24. 共通鍵暗号方式
暗号化と復号で同じ鍵を使用する暗号方式。通信相手ごとに異なる共通鍵が必要である。暗号化や復号に要する処理時間は、公開鍵暗号方式よりも短い。

25. AES（Advanced Encryption Standard）
米国の次世代暗号方式とし NIST（National Institute of Standards and Technology）によって規格された共通鍵暗号方式。

26. 公開鍵暗号方式
暗号化と復号に異なる鍵を使用する暗号方式。暗号化鍵は誰もが使用できるように公開し（公開鍵）、復号鍵は受信者が厳重に管理する（秘密鍵）。

27. RSA（Rivest Shamir Adleman）
公開鍵暗号のひとつ。桁数が大きい数の素因数分解が困難であることを利用している。

28. ハイブリッド暗号方式
公開鍵暗号方式における鍵管理の利便性と、共通鍵暗号方式の速い処理速度を組み合わせた方式。

29. ディジタル署名
公開鍵暗号技術を応用して文書の正当性を保証するために付けられる暗号化された署名情報のこと。この技術を利用すると、発信元の正当性と改ざんの有無が確認できる。

30. 認証局（CA、Certification Authority）
公開鍵暗号方式を用いたデータ通信において、利用者の公開鍵の正当性を保証するためのディジタル証明書を発行する第三者機関。

31. WPA2（Wi-Fi Protected Access 2）
無線 LAN を利用するときの主なセキュリティ方式のひとつ。暗号化アルゴリズム AES を利用している。

32. S/MIME（Secure MIME）
電子メールソフトに暗号技術を使ったセキュリティ機能を提供する技術。本文の暗号化に共通鍵暗号方式を用い、共通鍵の受渡しには公開鍵暗号方式を用いる。

33. PKI（Public Key Infrastructure）／公開鍵基盤
所有者と公開鍵の対応付けをするのに必要なポリシや技術の集合によって実現される基盤。

〔問題集〕

- ✓ **石川敢也「情報処理教科書 iパスクイズ 222 IT パスポート試験攻略の書」 翔泳社**
- ✓ **IT パスポート試験合格講座** http://rakupass.com/itpassport/