情報セキュリティマネジメント試験合格講座 09

- 情報セキュリティ対策

1. 組織における内部不正防止ガイドライン
   内部不正対策の整備を可能とすることを目的として、内部不正防止の重要性や対策の体制、関連する法律などの概要を IPA がまとめたガイドライン。

2. need to know の原則
   秘密に接する権限は、内容を知る必要のある人のみに限定されるという考え方。

3. RASIS(レイシス)
   システムの性能を評価する 5 つの概念の頭文字。

   - ✓ Reliability(信頼性):システムが故障を起こしにくい程度。
   - ✓ Availability(可用性):必要な時に使用可能状態にある割合。
   - ✓ Serviceability(保守性):システム障害時の修理し易さの程度。
   - ✓ Integrity(完全性):保存されているデータが完全である割合。
   - ✓ Security(安全性、機密性):データの障害に対する耐性の程度。

4. 脆弱性検査
   攻撃者の視点から様々な疑似攻撃を試行して、潜在的な脆弱性を発見し、安全性を調査・判定するセキュリティ診断。用いられるソフトウェアは「脆弱性検査ツール(VS、Vulnerability Scanner)」と呼ばれる。

5. ファジング(Fuzzing)
   問題を引き起こしそうな多様なデータを自動生成して入力し、ソフトウェアの応答や挙動から脆弱性を検出する検査手法。

6. ペネトレーションテスト
   侵入検査。コンピュータやネットワークのセキュリティ上の脆弱性を発見するために、システムを実際に攻撃して侵入を試みる検査手法。

Copyright © RakuPass.Com - Kanya Ishikawa All Rights Reserved.

7. DMZ（DeMilitarized Zone）
ネットワークにおいて外部と内部の間の隔離領域。ファイアウォールを設置することで、インターネットからもイントラネットからもアクセス可能だが、イントラネットへのアクセスを禁止しているネットワーク上の領域。

8. 検疫ネットワーク
セキュリティに問題があるPCを社内ネットワークなどに接続させないことを目的とした仕組みであり、外出先で使用したPCを会社に持ち帰った際に、ウイルスに感染していないことなどを確認するために利用するネットワーク上の領域。

9. WAF(Web Application Firewall)
Webアプリケーションの脆弱性を悪用する攻撃に含まれる可能性が高い文字列を定義し、攻撃であると判定した場合には、その通信を遮断する仕組み。

10. ベイジアン（Bayesian）フィルタリング
利用者が振り分けた迷惑メールから特徴を学習して迷惑メールであるかどうかを統計的に解析して判定する、学習型のスパムフィルタ。

11. パケットフィルタリング型ファイアウォール
インターネットなどの外部ネットワークと内部ネットワークの境界において、パケットのIPアドレスによって通過させるか遮断するかを判断する仕組み。

12. リバースプロキシ（Reverse Proxy）
ユーザ認証の役割などを持たせた特定のサーバを経由しなければならないように設置された代理サーバ。パスワードの代わりにディジタル証明書を使った認証も可能になる。

13. IPsec（Security Architecture for Internet Protocol）
インターネットで暗号化された通信を行うための手法。トランスポートモードでは、トンネルモードを使用すると、ゲートウェイ間の通信経路上だけではなく、発信側システムと受信側システムとの間の全経路上でメッセージが暗号化される。

14. IKE(Internet Key Exchange)
UDP（User Datagram Protocol）ポート番号500で通信するIPsec標準の鍵交換プロトコル。

Copyright © RakuPass.Com - Kanya Ishikawa All Rights Reserved.

15. SPF（Sender Policy Framework）
メール送信のなりすましを検知するために、差出人のメールアドレスが他のドメイン名になりすましていないかどうか、送信側ドメインの DNS サーバに問い合わせて確認する認証技術。

16. インベントリ（Inventory）収集
業務に無関係なソフトウェアがインストールされていることを検出するクライアント管理ツールやツール。

17. LDAP（Lightweight Directory Access Protocol）
ネットワーク上にある情報を管理するディレクトリデータベースへアクセスするためのプロトコル。

18. IDS(Intrusion Detection System)
侵入検知システム。パケットを監視し OS やミドルウェアのセキュリティホールを突いた攻撃を検知する。ネットワークを監視する NIDS(Network Based IDS、ネットワーク型 IDS)とサーバを監視する HIDS(Host Based IDS、ホスト型 IDS)がある。HIDS はシグネチャとのパターンマッチングを失敗させるためのパケットが挿入された攻撃でも検知できる。

19. NIDS(Network Intrusion Detection System)
ネットワーク型侵入検知システム。ネットワーク内への不正侵入の試みを検知し、管理者に通知する機能がある。

20. IPS（Intrusion Prevention System）
侵入防止システム。ネットワークやコンピュータへの不正侵入を防御する仕組み。

21. DNSSEC(DNS Security Extensions)
名前解決要求に対して応答を返す DNS サーバが、ディジタル署名を付加して送信することで、応答レコードが、正当であり、改ざんされていないことの検証を可能にする方式。

22. SSL アクセラレータ（Secure Sockets Layer Accelerator）
Web サーバの CPU 負荷を軽減するために、SSL による暗号化と復号の処理を行う専用のハードウェア。

Copyright © RakuPass.Com - Kanya Ishikawa All Rights Reserved.

23. SIEM（Security Information and Event Management）
セキュリティ情報イベント管理。ハードウェアやソフトウェアの複数のログをリアルタイムに管理して、セキュリティの脅威を検知したり、管理者に通知したりする仕組み。

24. ディジタルフォレンジックス（Digital Forensics）
情報セキュリティに関する犯罪に対する法的な根拠を明らかにして保全することや、そのための方法。Forensics は「科学捜査の」という意味。

25. ディジタルウォーターマーク（電子透かし）
画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む方法。

26. ステガノグラフィ（Steganography）
画像などのデータの中に、秘密にしたい情報を他者に気付かれることなく埋め込む方法。

27. ポリモーフィック型（Polymorphic）ウイルス
感染するごとにウイルスのコードを異なる鍵で暗号化し、同一のパターンで検知されないようにするタイプのウイルス。Polymorphic は「多形性の」という意味。

28. ハニーポット（Honey Pot）
侵入者をおびき寄せるために本物そっくりのシステムを設置し、侵入者の挙動などを監視する仕組み。

29. サンドボックス(Sandbox)
プログラムの外部を呼び出す機能を制限・遮断することで、システム全体に影響を与えないようにした仕組み。隔離された作業領域を指す用語。

〔問題集〕

✓ 石川敢也(共著)「情報セキュリティマネジメント要点整理＆予想問題集」 翔泳社
✓ 情報セキュリティマネジメント試験合格講座 http://rakupass.com/security/

Copyright © RakuPass.Com - Kanya Ishikawa All Rights Reserved.