1. 利用者が必要な時に情報資産を使えることは可用性、と言います。特定バックアップなどで向上させることができます。
2. リスク保有は、対策を講じないでリスクをそのままにしておくことで、損失額も発生率も小さくリスクに対して行う対策です。

3. PC が参照する DNS サーバに誤ったドメイン管理情報を覚え込ませて、偽のサーバに誘導する攻撃を DNS キャッシュポイズニングと言います。

4. LAN などの内部ネットワークとインターネットなどの外部ネットワークの間に配置し、LAN へ不正なアクセスができないようにするシステムをファイアウォールといいます。

5. キーロガーは、もともと利用者をサポートするためには、キーボード入力を監視して記録するソフトウェアです。

6. リスク回避は、リスクの原因を排除することで、損失額が大きく発生率の高いリスクに対して行う対策。

7. 管理者該当していないパスで Web サーバ内のファイルを指定し、許可されていないファイルを不正に閲覧する攻撃をディレクトリトラバーサルと言います。

8. 盗んだ ID やパスワードなどを使い、ネットワーク上でその人のふりをすることをなりすましと言います。

9. 銀行などを装った偽のウェブサイトを作り、URL を載せた電子メールを送り、ユーザにアクセスさせて暗証番号やパスワードをだまし取ることをフィッシ ングといいます。

10. Web アプリケーション上で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改ざんしたり不正に取得したりする攻撃を SQL インジェクションと言います。

1. リスク対応のうち、リスクの軽減に該当するものはどれか。

✨損失の発生率を低下させること

2. ファイアウォールのパケットフィルタリング機能に関する記述のうち、適切なものはどれか。

✨特定の TCP ポート番号を持ったパケットだけに、インターネットから内部ネットワークへの通過を許可する。

3. 情報セキュリティにおける"機密性"を脅かす攻撃はどれか。

✨システム内に保管されているデータの不正コピー

4. バイオメトリクス認証には、身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

✨署名するときの速度や筆圧から特徴を抽出して認証する。

5. リスク対応のうち、リスク共有（リスク移転）に該当するものはどれか。

✨保険への加入などで、他者との間でリスクを分散すること

6. 情報漏えい対策に該当するものはどれか。

✨ノート型 PC のハードディスクの内容を暗号化する

7. リスク対応のうち、リスク回避に該当するものはどれか。

✨リスクの原因を除去すること

8. WAF（Web Application Firewall）を利用する目的はどれか。

✨Web サーバ及び Web アプリケーションに起因する脆弱性への攻撃を遮断する。

9. SQL インジェクション攻撃による被害を防ぐ方法はどれか。

✨入力に上位ディレクトリを指定する文字列が含まれているときは受け付けない。

10. ディレクトリトラバーサル攻撃を防ぐ方法はどれか。

✨入力された文字が、データベースへの問合せや操作ににおいて、特別な意味を持つ文字として解釈されないようにする。