

Certificate of Cloud Security Knowledge (V4.0) Exam (CCSK Japanese Version)

1. すべての資産は、クラウド内で同じ継続性を必要とします。

A. 真

B. いいえ

Answer(s): B

2. 監査は、ベスト プラクティス、適切なリソース、およびテスト済みのプロトコルと標準を反映するように堅牢に設計する必要があります。また、どのタイプの監査人を使用する必要がありますか？

A. 会計監査人

B. 上記のいずれでもない

C. クラウド プロバイダーの利益のために働く監査人

D. クラウドの顧客の利益のために働く監査人

E. CSA認定

Answer(s): A

3. クラウド プロバイダーとのコンプライアンスの整合性とギャップを理解するために、クラウドの顧客は何に依存する必要がありますか？

A. EDiscovery ツール

B. プロバイダーと消費者の契約

C. 第三者認証

D. プロバイダーのドキュメント

E. プロバイダーの実行監査とレポート

Answer(s): C

4. 個別の仮想ネットワーク上でアプリケーションを実行し、必要なネットワークのみを接続することはどのように役立ちますか？

A. ハードウェア コストを削減します。

B. 侵害されたシステムの爆発範囲を縮小します

C. アクセスをロックダウンし、より強力なデータ セキュリティを提供します。

D. ビジネス グループを中心にアプリケーションを構成できます。

E. 管理オーバーヘッドが少ない動的で詳細なポリシーを提供します。

Answer(s): B

5. クラウド環境全体でのデータ検索について正しいのはどれですか？

A. ホストされているすべてのデータを検索またはアクセスする機能または管理者権限がない可能性があります。

B. E-Discovery ツールを使用して、環境全体を簡単に検索できます。

C. クラウド プロバイダーは、完全な管理コントロールで検索を実行する必要があります。

D. 検索と発見の時間は、コンシューマーとプロバイダーの間の契約に常に考慮されます。

E. クラウドでホストされているすべての電子メール アカウントは簡単に検索できます。

Answer(s): A

6. 2 つ以上の固有のクラウドのクラウド展開は、次のように呼ばれます。

A. プライベート クラウド

B. コミュニティ クラウド

C. ハイブリッド クラウド

D. ジェリコ クラウド キューブ モデル

E. サービスとしてのインフラストラクチャ

Answer(s): B

7. 次の項目のうち、Security as a Service (SecaaS) の例ではないものはどれですか？

A. プロビジョニング

B. 認証

C. 迷惑メールフィルタリング

D. Web フィルタリング

E. 侵入検知

Answer(s): A

8. クラウド セキュリティの実装に役立つ一般化されたテンプレートを提供するクラウド セキュリティ モデル タイプはどれですか？

A. クラウド コントロール マトリックス (CCM)

B. 概念モデルまたはフレームワーク

C. 参照アーキテクチャ

D. モデルまたはフレームワークを制御します

E. デザインパターン

Answer(s): C

9. セキュリティを強化するために、データの断片化とともにどのような方法を利用できますか？

A. 組織

B. 絶縁

C. 暗号化

D. ナレッジマネジメント

E. IDS

Answer(s): B

10. 組織におけるクラウド ガバナンスの主な目的は何ですか？

A. クラウド環境内でのデータ転送速度を向上させる

B. クラウドサービスのコストを削減する

C. 組織の目標に沿ったコンプライアンス、セキュリティ、効率的な管理を確保する

D. オンプレミスのデータセンターの必要性を排除する

Answer(s): C

11. クラウド セキュリティ インシデントを処理する際に考慮すべき重要な点は何ですか？

A. ネットワークトラフィックの監視

B. 技術的な修正に焦点を当てる

C. クラウド サービス プロバイダーのサービス レベル契約

D. 追加のスタッフの雇用

Answer(s): C

12. Software Defined Perimeter (SDP) にはどのコンポーネントが含まれていますか？

A. クライアント、コントローラー、およびファイアウォール

B. コントローラー、ファイアウォール、およびゲートウェイ

C. クライアント、ファイアウォール、およびゲートウェイ

D. クライアント、コントローラー、およびゲートウェイ

E. クライアント、コントローラー、ファイアウォール、およびゲートウェイ

Answer(s): D

13. 次のステートメントのうち、クラウド環境におけるガバナンスとエンタープライズ リスク管理の要件ではないものはどれですか？

A. クラウド サプライ チェーンの他のメンバーから継承されたリスクを検査して説明し、運用上の回復力によってリスクを軽減および封じ込めるための積極的な対策を講じます。

B. クラウド環境の一時的な性質を回避するために、十分に吟味されたソフトウェア アプリケーションを使用する企業と長期契約を交渉します。

C. B と C の両方。

D. 財務上のソルベンシーと組織の透明性を示すステークホルダーと株主に透明性を提供します。

E. クラウド サプライ チェーンに内在するリスクの相互依存性を尊重し、企業のリスク体制と準備状況を消費者と依存関係者に伝えます。

Answer(s): B

14. 多要素認証 (MFA) が ID ベースの攻撃の防止にどのように役立つかを最もよく説明しているのは次のどれですか。

A. MFA は、アカウントを保護するために物理的なトークンと生体認証に依存します。

B. MFA では複数の形式の検証が必要であり、妥協が必要になります。

C. MFA では、アカウントを保護するために、より複雑なパスワードが必要となり、それを使用します。

D. MFA はシングル サインオンを通じてパスワードの必要性を排除します。

Answer(s): B

15. ENISA: 「VM ホッピング」とは:

A. 侵害された VM を使用してハイパーバイザーを悪用し、他の VM を制御するために使用されます。

B. VM インスタンスの不適切な管理により、お客様の VM が他のお客様のシステムと混在する原因となります。

C. 脆弱性管理基準の欠如。

D. 仮想ルーティング システム内でのループ。

E. VM パッチ管理が不安定で、VM ルーティング エラーが発生しています。

Answer(s): A

16. メタストラクチャーに接続してクラウド環境を構成するために使用されるインターフェースとして知られているものは何ですか？

A. 管理プレーン

B. シングルサインオン

C. ID およびアクセス管理

D. 管理アクセス

E. クラウド ダッシュボード

Answer(s): A

17. システムまたは環境がテンプレートから自動的に構築されるとはどういう意味ですか？

A. 本番環境で行われた変更は、次のコードまたはテンプレートの変更によって変更されません。

B. 本番環境で行われた変更は、次のコードまたはテンプレートの変更によって上書きされます。

C. 何もありません。

D. 自動化の構成によって異なります。

E. テストで行われた変更は、次のコードまたはテンプレートの変更によって上書きされます。

Answer(s): E

18. クラウドベースのリソースへのアクセス レベルを決定するために使用される、トランザクション内のエンティティのクレームと属性で構成される一連の定義ルールは何と呼ばれますか？

A. 検証プロセス

B. サポートテーブル

C. 資格マトリックス

D. アクセスログ

E. エントリーログ

Answer(s): A

19. ENISA: すべてのシナリオに共通する 5 つの主要な法的問題の 1 つではないものは次のとおりです。

A. 知的財産

B. データ保護

C. グローバル化

D. 業務上の過失

E. アウトソーシング サービスとコントロールの変更

Answer(s): C

20. CCM: CCM ツールでは、a はリスクを修正する尺度であり、リスクを修正するプロセス、ポリシー、デバイス、プラクティス、またはその他のアクションが含まれます。

A. リスク影響

B. コントロール仕様

C. ドメイン

Answer(s): B
