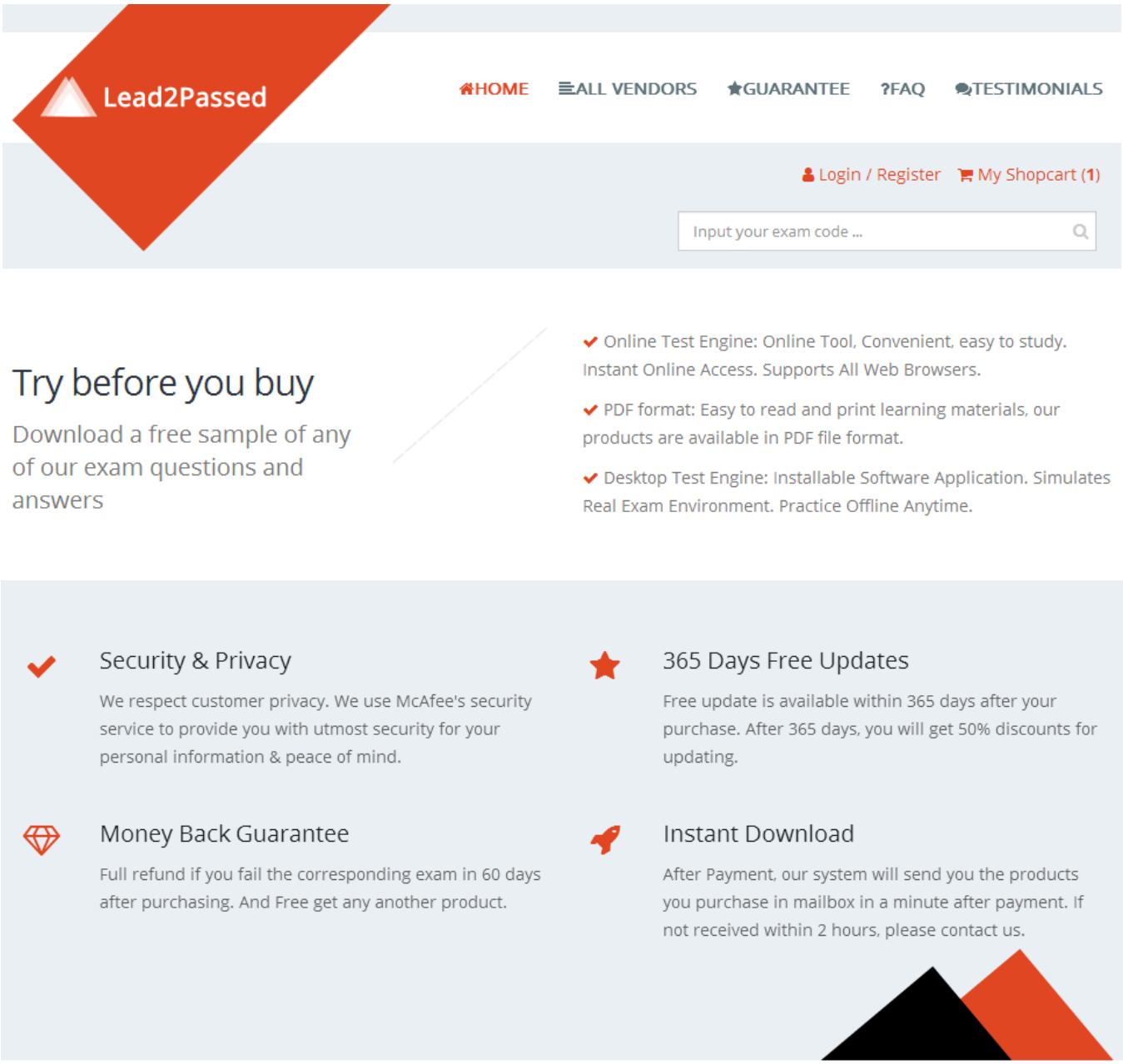
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

Exam : **CCSP-JPN**

Title : Certified Cloud Security Professional (CCSP日本語版)

Vendor : ISC

Version : DEMO

QUESTION NO: 1
SaaS環境内の次のタスクのうち、クラウドの顧客が責任を負わないものはどれですか？
A.認証メカニズム
B.ブランディング
C.トレーニング
D.ユーザーアクセス
Answer: A
Explanation:
The authentication mechanisms and implementations are the responsibility of the cloud provider because they are core components of the application platform and service. Within a SaaS implementation, the cloud customer will provision user access, deploy branding to the application interface (typically), and provide or procure training for its users.

QUESTION NO: 2
ユーザーアカウント/アクセスのレビューとメンテナンスに誰が関与する必要がありますか？
A.ユーザーのマネージャー
B.セキュリティマネージャー
C.経理部
D.インシデント対応チーム
Answer: A

QUESTION NO: 3
次の用語のうち、リスク許容の一般的に使用されるカテゴリではないものはどれですか？
A.中程度
B.クリティカル
C.最小限
D.受け入れ
Answer: D
Explanation:
Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

QUESTION NO: 4
米国国務省は、技術輸出として知られているものとして何を管理していますか？
A.DRM
B.ITAR
C.EAR
D.EAL
Answer: B
Explanation:
ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

QUESTION NO: 5
クラウド構成での監視とテストの責任を共有するために、プロバイダーはこれらすべてをクラウド顧客に提供する場合があります。
A.監査ログとパフォーマンスデータへのアクセス
B.DLPソリューションの結果
C.セキュリティ管理
D.SIM、SEIM。およびSEMログ
Answer: C
Explanation:
While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

QUESTION NO: 6
システムまたはアプリケーションが従わなければならない規制の背後にある主な要因は次のうちどれですか？
A.データソース
B.地域
C.契約
D.SLA
Answer: B
Explanation:
The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

QUESTION NO: 7
ファイルシステムレベルで暗号化を使用する以外に、オブジェクトストレージシステムに格納されているデータを保護するために最も広く使用されているテクノロジーはどれですか。
A.TLS
B.HTTPS
C.VPN
D.IRM
Answer: D
Explanation:
Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through

traditional control mechanisms. Hypertext Transfer Protocol Secure (HTTPS), virtual private network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services and likely will be used in conjunction with other object data protection strategies.

QUESTION NO: 8
クラウドシステムは、組織のBCDRソリューションにますます使用されています。
クラウドコンピューティングのどの側面がBCDRの使用を最も魅力的にしていますか？
A.オンデマンドのセルフサービス
B.測定サービス
C.移植性
D.幅広いネットワークアクセス
Answer: B
Explanation:
Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed.
This traditionally has led to increased costs for an organization because physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers.
Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case.
On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

QUESTION NO: 9
次のストレージタイプのうち、従来のファイルシステムとツリー構造に最も密接に関連しているのはどれですか。
A.ボリューム
B.非構造化
C.オブジェクト
D.構造化
Answer: A
Explanation:
Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

QUESTION NO: 10
アプリケーションまたはシステムの要件収集への入力として含まれないのは、次のうちどれですか？
A.ユーザー

B.管理
C.規制当局
D.監査人
Answer: D

QUESTION NO: 11
監査範囲ステートメントは、監査の制限と結果を定義します。
監査範囲ステートメントの一部として含まれないものは次のうちどれですか？
A.レポート
B.認証
C.請求
D.除外
Answer: C
Explanation:
Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors.
Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

QUESTION NO: 12
次のセキュリティの側面のうち、クラウドプロバイダーの責任はどれですか。
A.規制遵守
B.物理的なセキュリティ
C.オペレーティングシステムの監査
D.開発者の個人的なセキュリティ
Answer: B
Explanation:
Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

QUESTION NO: 13
認定と規格が異なれば、データセンターの設計と運用に対するアプローチも異なります。多くの従来のアプローチは段階的な方法論を使用していますが、次のうちどれがデータセンターの設計にマクロレベルのアプローチを利用していますか？
A.IDCA
B.BICSI
C.Uptime Institute
D.NFPA

Answer: A
Explanation:
The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities.
The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

QUESTION NO: 14
TLSが使用する2つのプロトコルは何ですか？
A.ハンドシェイクと記録
B.転送して開始
C.ハンドシェイクとトランスポート
D.記録して送信
Answer: A
Explanation:
TLS uses the handshake protocol to establish and negotiate the TLS connection, and it uses the record protocol for the secure transmission of data.

QUESTION NO: 15
SLAには、契約のパフォーマンスとクラウドプロバイダーとクラウドカスタマー間の満足度に関する公式の要件が含まれています。
SLAの一部として測定可能なメトリックと要件を持つコンポーネントではないものは次のうちどれですか？
A.ネットワーク
B.ユーザー
C.メモリ
D.CPU
Answer: B
Explanation:
Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically.
However, user access and user experience would be covered indirectly through other metrics.
Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

QUESTION NO: 16
組織には、BCDRの状況を活性化するために業界全体で共通する多くの理由が考えられます。次のうち、BCDRプランをアクティブ化する一般的な理由ではないものはどれですか？
A.自然災害

B.ユーティリティの停止
C.スタッフの損失
D.テロ攻撃
Answer: C

QUESTION NO: 17
使用しているクラウドモデルに関係なく、クラウドのお客様の責任は次のうちどれですか。
A.インフラストラクチャ
B.プラットフォーム
C.アプリケーション
D.データ
Answer: D
Explanation:
Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

QUESTION NO: 18
クラウドBC /
DRアクティビティで一般的に利用可能なさまざまなモデルには、以下を除くすべてが含まれます。
A.プライベートアーキテクチャ、クラウドバックアップ
B.クラウドプロバイダー、別のクラウドプロバイダーからのバックアップ
C.クラウドプロバイダー、同じプロバイダーからのバックアップ
D.クラウドプロバイダー、プライベートプロバイダーからのバックアップ
Answer: D
Explanation:
This is not a normal configuration and would not likely provide genuine benefit.

QUESTION NO: 19
あなたは政府の研究施設で働いています。あなたの組織は、他の政府の研究組織とデータを共有することがよくあります。
組織全体でシングルサインオンエクスペリエンスを作成し、各組織のユーザーがその組織によって発行されたユーザーID
/認証を使用してサインインし、他のすべての組織の調査データにアクセスできるようにします。
各組織のデータストアを他のすべての組織に複製するのではなく（これは、この目標を達成する1つの方法です）、代わりに、すべてのユーザーが各組織の特定のストレージリソースにアクセスできるようにします。
組織間で各ユーザーのユーザーIDと認証資格情報を渡すために、どのプロトコル/言語/モチーフを利用する可能性が最も高いですか？
応答：
A. Representational State Transfer (REST)
B. Security Assertion Markup Language (SAML)
C. Simple Object Access Protocol (SOAP)

D. Hypertext Markup Language (HTML)
Answer: B

QUESTION NO: 20
クラウド環境にいるクラウドユーザーは、データの保存方法とシステムの展開方法に関する多くの洞察と知識を失っています。
ISO /
IECクラウド標準のどの概念が、これらの問題についてクラウドの顧客に情報を提供するクラウドプロバイダーの必要性に関連していますか？
A.開示
B.透明度
C.開放性
D.ドキュメント
Answer: B
Explanation:
Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

QUESTION NO: 21
あなたは監査スコープステートメントの作成を任されており、プロジェクトの概要を作成しています。次のうち、監査スコープステートメントに通常含まれないものはどれですか？
A.目的の声明
B.成果物
C.分類
D.コスト
Answer: D

QUESTION NO: 22
次のうち、クラウドセキュリティアライアンスによって公開されたクラウドコントロールマトリックス内で定義されたセキュリティコントロールドメインの1つではないものはどれですか？
A.財務
B.人材
C.モバイルセキュリティ
D.IDおよびアクセス管理
Answer: A

QUESTION NO: 23
TLSの一部として、どのプロトコルが実際の安全な通信とデータの送信を処理しますか？
A.交渉
B.ハンドシェイク
C.転送

D.レコード
Answer: D
Explanation:
The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for encrypting and authenticating packets throughout their transmission between the parties, and in some cases it also performs compression. The TLS handshake protocol is what negotiates and establishes the TLS connection between two parties and enables the secure communications channel to then handle data transmissions. Negotiation and transfer are not protocols under TLS.

QUESTION NO: 24
次のストレージタイプのうち、Infrastructure as a
Service（IaaS）ソリューションで使用されているのはどれですか？
A.ボリュームとブロック
B.構造化されたオブジェクト
C.構造化されていない一時的な
D.ボリュームとオブジェクト
Answer: D

QUESTION NO: 25
以下はすべて、クラウドデータの移植性を向上させ、ベンダーロックインの可能性を最小限に抑えるための手法です。
A.引っ越しに物理的な制限がないことを確認します
B.クラウド運用全体で広くDRMおよびDLPソリューションを使用する
C.移植性をサポートするために有利な契約条件を確保する
D.独自のデータ形式を避ける
Answer: B
Explanation:
DRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

QUESTION NO: 26
BCDRテストを定期的に実行することは、プロセスとドキュメントが依然として関連性があり効率的であることを確認するためのベストプラクティスですが、定期的な間隔外でBCDRレビューを実施する理由を表すものは次のうちどれですか。
A.スタッフの変更
B.アプリケーションの変更
C.規制の変更
D.管理の変更
Answer: B

QUESTION NO: 27
クラウドの顧客がクラウド環境内で使用するリソースとオファリングにのみ支払い、それらを消費している間のみ支払う、次の概念のどれですか？

A.消耗品サービス
B.測定サービス
C.請求可能なサービス
D.従量制サービス
Answer: B
Explanation:
Measured service is where cloud services are delivered and billed in a metered way, where the cloud customer only pays for those that they actually use, and for the duration of time that they use them.

QUESTION NO: 28
クラウドデータセンターキャンパスの物理的なレイアウトには、_____を除く次のすべての冗長性を含める必要があります。
A.物理的な境界セキュリティ制御（フェンス、ライト、壁など）
B.管理/サポートスタッフの構築
C.電気事業ライン
D.通信接続線
Answer: B

QUESTION NO: 29
オンプレミス環境からホスト型クラウドサービスに移行するオプションを検討する場合、組織は、外部エンティティがコラボレーション目的でクラウドデータにアクセスできるようにするリスクを_____と比較検討する必要があります。
A.レガシー環境でデータを保護していません
B.データを公開する
C.コラボレーションを強化するために外部の担当者をレガシーワークスペースに招待する
D.コラボレーションの目的でレガシー環境の外部にデータを送信する
Answer: D

QUESTION NO: 30
クラウドの分野横断的な側面のどれが、ジョブ、タスク、および役割の割り当てに関連し、それらが成功し、適切に実行されることを保証することに関連していますか？
A.サービスレベル契約
B.ガバナンス
C.規制要件
D.監査能力
Answer: B
Explanation:
Governance at its core is the idea of assigning jobs, takes, roles, and responsibilities and ensuring they are satisfactory performed.

QUESTION NO: 31
ビジネス継続性と災害復旧はどのセキュリティ概念に該当しますか？
A.守秘義務

B.可用性
C.フォールトトレランス
D.完全性
Answer: B
Explanation:
Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

QUESTION NO: 32
動的アプリケーションセキュリティテスト（DAST）は通常、_____形式のテストと見なされます。
応答：
白い箱
A.乾いた畑
B.ブラックボックス
C.グレーボックス
D.乾いた畑
Answer: B

QUESTION NO: 33
TLSは、_____通信に_____を提供します。
A.プライバシー、セキュリティ
B.セキュリティ、最適化
C.プライバシー、完全性
D.強化、プライバシー
Answer: C

QUESTION NO: 34
SOCタイプ2レポートは5つの原則に分かれています。
他の4つの原則のいずれかを監査する場合、5つの原則のうちどれを含める必要がありますか？
A.守秘義務
B.プライバシー
C.セキュリティ
D.可用性
Answer: C
Explanation:
Under the SOC guidelines, when any of the four principles other than security are being audited, which includes availability, confidentiality, processing integrity, and privacy, the security principle must also be included with the audit.

QUESTION NO: 35
Cloud Security Alliance Cloud Controls Matrix（CCM）とは何ですか？
A.クラウドサービスプロバイダーのソフトウェア開発ライフサイクル要件のセット
B.セキュリティドメインの階層に配置されたクラウドサービスセキュリティコントロールの一覧
C.個別のセキュリティドメインに配置されたクラウドサービスセキュリティコントロールの一覧
D.クラウドサービスプロバイダーの一連の規制要件
Answer: C
Explanation:
The CSA CCM is an inventory of cloud service security controls that are arranged into separate security domains, not a hierarchy.