Actual4Dump

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.actual4dump.com

Superb Exam Dumps Materials lead you to get your certification easily - Actual4dump

Exam : **CC-JPN**

Title : Certified in Cybersecurity (CC) (CC日本語版)

Vendor : ISC

Version : DEMO

QUESTION NO: 1
デジタル署名によって保証されない特性は次のどれですか
A. 認証
B. 機密保持
C. 否認防止
D. 誠実さ
Answer: B
Explanation:
Digital signatures provideauthentication,integrity, andnon-repudiation, but they donot provide confidentiality.
A digital signature verifies who sent the message and ensures it was not altered, but the content remains readable unless encryption is also applied.
Confidentiality requires encryption, typically using symmetric or asymmetric cryptography.
Digital signatures are often combined with encryption (such as in TLS or secure email), but by themselves they do not hide message contents.

QUESTION NO: 2
HTTPS ではどのようなセキュリティ機能が使用されていますか?
A. IPSec
B. SSH
C.ICMP
D. SSL/TLS
Answer: D
Explanation:
HTTPS uses SSL/TLS to provide encryption, authentication, and integrity for web communications.

QUESTION NO: 3
物理トポロジを変更せずにネットワークを論理的にセグメント化するためにスイッチによって作成されます。
A. LAN
B. WAN
C. VLAN
D. MAN
Answer: C
Explanation:
VLANslogically separate networks at Layer 2 while sharing the same physical infrastructure.

QUESTION NO: 4
地理的に分散しているにもかかわらず、同じ LAN
上にあるように見えるワークステーション、サーバー、およびネットワーク
デバイスの論理グループ。
A. LAN
B. VPN

C. WLAN
D. VLAN
Answer: D
Explanation:
A Virtual Local Area Network (VLAN) is a logical segmentation of network devices that allows systems to appear as though they are on the same local network, regardless of their physical location. VLANs operate at the Data Link layer (Layer 2) and use tagging (such as IEEE 802.1Q) to separate broadcast domains logically.
VLANs improve security, performance, and manageability by isolating traffic between different groups of systems. Devices in the same VLAN can communicate as if they were on the same LAN, even if they are physically distributed across different switches or buildings.
LAN refers to a physical local network, VPN provides encrypted tunnels across networks, and WLAN refers to wireless LANs. Only VLANs provide logical grouping independent of geography.

QUESTION NO: 5
VLAN ホッピングはどの OSI 層に属しますか?
A. レイヤー3
B. レイヤー4
C. レイヤー7
D. レイヤー2
Answer: D
Explanation:
VLAN hopping exploits weaknesses in Layer 2 switching mechanisms such as trunking and tagging.

QUESTION NO: 6
リスクを無視して事業運営を継続することは、次のように知られています。
A. リスク受容
B. リスク軽減
C. リスク回避
D. リスク移転
Answer: A
Explanation:
Risk acceptance acknowledges the risk and chooses to proceed without additional controls, often due to cost or low impact.

QUESTION NO: 7
組織はどのくらいの頻度で BCP をテストする必要がありますか?
A. 継続的に
B. 毎年
C. 日常的に
D. 毎日
Answer: C

Explanation:
BCPs should be testedroutinely(e.g., tabletop, simulations) to ensure readiness and relevance.

QUESTION NO: 8
登録されたポートは主に何に使用されますか?
A. コアTCP/IPプロトコル
B. Webサーバー
C. 社内アプリケーション
D. ベンダーおよび独自アプリケーション
Answer: D
Explanation:
Registered ports (1024-49151) are typically assigned to vendor-specific or proprietary applications, such as database services.

QUESTION NO: 9
送信元アドレスを偽装して不正侵入する行為は次のように呼ばれます。
A. フィッシング
B. ARP
C. なりすまし
D. すべて
Answer: C
Explanation:
Spoofing involves falsifying identity information (IP, MAC, email headers) to appear as a trusted source and bypass controls.

QUESTION NO: 10
個人を特定できる情報 (PII) とは何ですか?
A. 個人の健康状態に関する情報
B. 個人を特定できる可能性のある個人に関するデータ
C. 企業秘密、研究、事業計画、知的財産
D. 情報の所有者によって割り当てられた重要性
Answer: B
Explanation:
Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual, either directly or indirectly. Examples include full name, Social Security number, date of birth, address, email address, phone number, and biometric identifiers.
PII is regulated by numerous laws and standards, including privacy regulations and data protection frameworks. Protecting PII is critical to prevent identity theft, fraud, and privacy violations.
Health information is a subset of sensitive data (often classified as PHI). Trade secrets and business data fall under intellectual property. Information classification levels describe value, not identity.
Security controls for PII typically include encryption, access control, monitoring, and data loss

prevention mechanisms.

QUESTION NO: 11
リスク管理プロセスの最初のステップは何か
A. リスク対応
B. リスク軽減
C. リスクの特定
D. リスク評価
Answer: C
Explanation:
Risk identification is the first step in the risk management process. Organizations must first identify assets, threats, and vulnerabilities before they can assess likelihood or impact. Without knowing what risks exist, meaningful assessment and mitigation are impossible.

QUESTION NO: 12
ユーザーは、必要なタスクを実行するために必要な特定のデータとリソースにのみアクセスできる必要があると規定している原則はどれですか。
A. ゼロトラスト
B. 多層防御
C. 最小権限
D. すべて
Answer: C
Explanation:
ThePrinciple of Least Privilegeensures users, applications, and systems have only the minimum permissions necessary to perform their duties. This reduces the attack surface and limits potential damage if credentials are compromised.

QUESTION NO: 13
モノリシックなセキュリティを回避するために、複数の種類のアクセス制御を階層的に使用します。
A. DMZ
B. VLAN
C. 多層防御
D. VPN
Answer: C
Explanation:
Defense in Depth employs administrative, technical, and physical controls across multiple layers to reduce reliance on any single security mechanism. This approach increases resilience and detection capability.

QUESTION NO: 14
攻撃者にとって遠隔操作される「ロボット」のように動作する悪意のあるコード。
A. ルートキット
B. マルウェア

C. ボット
D. ウイルス
Answer: C
Explanation:
Abotis malware that allows attackers to remotely control infected systems, often forming botnets used for DDoS attacks, spam, or credential theft.

QUESTION NO: 15
Bell-LaPadula アクセス制御モデルは次の形式をとります。
A. RBAC
B. MAC
C. DAC
D. ABAC
Answer: B
Explanation:
Bell-LaPadula is a Mandatory Access Control (MAC) model focused on confidentiality. It uses security labels and clearances to enforce access rules such as "no read up, no write down."

QUESTION NO: 16
低、中、高などの記述子の割り当てに基づいたリスク分析の方法。
A. 定量的リスク分析
B. リスク評価
C. リスク軽減
D. 定性リスク分析
Answer: D
Explanation:
Qualitative risk analysis evaluates risk using descriptive categories such aslow,medium, andhighinstead of numerical values. This approach relies on expert judgment, experience, and contextual understanding rather than precise financial or statistical calculations.
According to NIST SP 800-30, qualitative analysis is especially useful when numerical data is unavailable or when rapid risk prioritization is required.
Unlike quantitative risk analysis, which assigns monetary values and probabilities, qualitative analysis focuses on relative severity and likelihood. It is commonly used during early stages of risk management, policy development, and executive decision-making. While less precise, qualitative risk analysis is easier to communicate to stakeholders and helps organizations focus resources on the most critical risks.

QUESTION NO: 17
会社のネットワークで突然のネットワークパケットの集中が発生し、インターネットトラフィックが大幅に低下しました。これはどのような種類のイベントですか？
A. セキュリティインシデント
B. 自然災害
C. エクスプロイト
D. 有害事象

Answer: D
Explanation:
A sudden flood of network packets causing degraded performance is best classified as anadverse event. An adverse event is any occurrence that negatively affects system performance, availability, or operations but may not yet meet the threshold of a confirmed security incident. According to NIST definitions, events such as traffic spikes, system slowdowns, or anomalous behavior are initially treated as adverse events until further analysis confirms malicious intent.
If investigation later confirms the flood was caused by a deliberate denial-of-service attack, the classification may escalate to asecurity incident. However, without confirmation of intent or compromise, adverse event is the most accurate term.

QUESTION NO: 18
データ侵害を防ぐために最も一般的に使用されるセキュリティ制御は何ですか?
A. 物理的な制御
B. 論理制御
C. 管理制御
D. RBAC
Answer: B
Explanation:
Logical (technical) controls such as encryption, access controls, DLP, and firewalls directly prevent unauthorized data access and exfiltration.

QUESTION NO: 19
個々のマシンやユーザーに至るまで、非常にきめ細かな制限を可能にするものはどれですか?
A. DMZ
B. マイクロセグメンテーション
C. VLAN
D. NAC
Answer: B
Explanation:
Microsegmentation enables fine-grained, software-defined security controls, limiting lateral movement within networks.

QUESTION NO: 20
情報の不正な開示、変更、破壊、または紛失によって予想される損害の規模は次のように表されます。
A. 脅威
B. 脆弱性
C. 影響
D. 可能性
Answer: C
Explanation:

Impact measures the severity of consequences if a security event occurs. It is a key component of risk calculations along with likelihood.

QUESTION NO: 21
動的承認の例
A. DAC
B. RBAC
C. MAC
D. ABAC
Answer: D
Explanation:
Attribute-Based Access Control (ABAC) is considered a dynamic authorization model because access decisions are made in real time based on attributes of the user, resource, action, and environment. These attributes can include time of day, device type, location, data sensitivity, and user role.
Unlike RBAC or MAC, which rely on static roles or labels, ABAC evaluates policies dynamically using a policy decision point (PDP). This makes ABAC ideal for modern cloud, zero trust, and highly distributed environments.
DAC allows owners to grant permissions, RBAC uses predefined roles, and MAC relies on fixed security labels. ABAC provides the most flexible and context-aware authorization.

QUESTION NO: 22
災害復旧の取り組みによく関連するアクティビティは何ですか?
A. マルウェア対策を実行中
B. 脆弱性スキャン
C. ゼロデイ攻撃
D. 従業員が主な生産拠点に戻る
Answer: D
Explanation:
Disaster Recovery includes restoring systems and returning operations to normal, which may involve staff moving back to the primary site after temporary relocation.

QUESTION NO: 23
誰もが遵守しなければならず、通常は違反した場合に金銭的な罰則が科せられる一連の規則は次のとおりです。
A. 標準
B. ポリシー
C. 手順
D. 法律または規制
Answer: D
Explanation:
Laws and regulations are legally enforceable and can impose fines or penalties. Standards and policies are not legally binding unless mandated by regulation.

QUESTION NO: 24
強力な事業継続プログラムによって強化されるセキュリティの目標は何ですか?
A. 否認防止
B. 在庫状況
C. 機密性
D. 誠実さ
Answer: B
Explanation:
Availability is the primary security goal enhanced by a strong business continuity program. Business continuity planning focuses on ensuring that critical systems, services, and operations remain accessible during and after disruptive events such as cyberattacks, natural disasters, or system failures.
Availability is one of the three pillars of the CIA triad and ensures that authorized users can access information and systems when needed. Business continuity strategies include redundancy, failover systems, backups, alternate processing sites, and disaster recovery plans.
While confidentiality and integrity are important, business continuity is primarily concerned with minimizing downtime and maintaining operational resilience. Non-repudiation relates to accountability and is not a continuity objective.
Frameworks such as NIST SP 800-34 and ISO/IEC 22301 emphasize availability as the core outcome of effective business continuity and disaster recovery planning.

QUESTION NO: 25
XenServer、LVM、Hyper-V、ESXi は次のとおりです。
A. タイプ2ハイパーバイザー
B. タイプ1ハイパーバイザー
C. 両方
D. なし
Answer: B
Explanation:
These areType 1 (bare-metal) hypervisors, running directly on hardware without a host operating system, offering higher performance and security.

QUESTION NO: 26
バッファオーバーフロー攻撃に必要な作業量を増やすには、どのテクノロジを実装する必要がありますか?
A. アドレス空間レイアウトのランダム化
B. 記憶誘導アプリケーション
C. 入力メモリの分離
D. 読み取り専用メモリの整合性チェック
Answer: A
Explanation:
Address Space Layout Randomization (ASLR) randomizes the memory locations used by applications, making it significantly harder for attackers to predict where malicious payloads

should be placed during buffer overflow attacks.
Buffer overflow exploits rely on predictable memory layouts. ASLR disrupts this predictability, increasing attacker effort and reducing exploit reliability.
The other options are either non-standard terms or unrelated to buffer overflow mitigation.
ASLR is widely used in modern operating systems and is a key defensive control recommended by secure coding and system hardening guidelines.
ASLR does not eliminate vulnerabilities but raises the attack complexity, which is a core defensive strategy.

QUESTION NO: 27
IT プロフェッショナルは、IT の問題とセキュリティ
インシデントをどのように区別するのでしょうか?
A. 医療援助
B. 証拠収集のみ
C. 専門的なインシデント対応トレーニング
D. 参加から学んだ教訓
Answer: C
Explanation:
Incident response training enables professionals to recognize malicious activity versus routine IT failures and respond appropriately.

QUESTION NO: 28
抑止制御の例はどれですか?
A. 生体認証
B. Guard dog
C. 暗号化
D. 回転式改札口
Answer: B
Explanation:
A guard dog deters unauthorized access by increasing perceived risk. Deterrent controls discourage attacks before they occur.

QUESTION NO: 29
ホストが利用可能かどうかを判断するために IETF によって RFC 792 を通じて標準化された IP ネットワーク プロトコルは次のとおりです。
A. IP
B. ICMP
C.IGMP
D. HTTP
Answer: B
Explanation:
ICMP is used for network diagnostics, including ping operations that test host availability. RFC 792 defines ICMP behavior.

QUESTION NO: 30
身体傷害賠償請求を避けるため、ある企業は高リスクのサービスを提供しないことに決定しました。これは次のような事例です。
A. リスク受容
B. リスク評価
C. リスク回避
D. リスク管理
Answer: C
Explanation:
Risk Avoidanceeliminates risk by discontinuing activities that expose the organization to unacceptable threats.

QUESTION NO: 31
セキュリティ
インシデントを検出し、対応し、回復するための一連の手順は次のとおりです。
A. BCP
B. IRP
C. DRP
D. なし
Answer: B
Explanation:
An Incident Response Plan (IRP) defines procedures for managing and mitigating security incidents.

QUESTION NO: 32
どの OSI レイヤーが MAC アドレスをネットワーク デバイスに関連付けますか?
A. 物理層
B. ネットワーク層
C. データリンク層
D. トランスポート層
Answer: C
Explanation:
The Data Link layer (Layer 2) handles MAC addressing and frame delivery within local networks.

QUESTION NO: 33
リスク特定の目的は次のとおりです。
A. あらゆるレベルの従業員がリスクの特定に協力する
B. リスクを特定し、明確に伝える
C. リスクを特定し、それらから保護する
D. すべて
Answer: D
Explanation:
Risk identification is a collaborative process that enables awareness, communication, and

protection against threats.

QUESTION NO: 34
ISC2 メール サーバーが他のメール サーバーにメールを送信する場合、 -? になります。
A. SMTPサーバー
B. SMTPピア
C. SMTPマスター
D. SMTPクライアント
Answer: D
Explanation:
When a mail server sends email to another mail server, it acts as anSMTP client. In the Simple Mail Transfer Protocol (SMTP), roles are defined by behavior, not by the system's primary function.
The sending system initiates the connection and issues SMTP commands, which makes it the client for that transaction. The receiving mail server listens for incoming connections and acts as the SMTP server.
Mail servers routinely switch roles depending on the direction of communication. A single system may act as an SMTP server when receiving mail and as an SMTP client when sending mail.
Understanding SMTP roles is important for configuring mail security controls such as firewalls, TLS enforcement, spam filtering, and authentication. Security professionals must recognize that "client" and
"server" are session-based roles, not permanent system identities.

QUESTION NO: 35
サーバールームに推奨される消火システムは何ですか?
A. フォームベース
B. 水性
C. 粉末ベース
D. クリーンエージェントガスシステム(例：FM-200 / Inergen)
Answer: D
Explanation:
Clean-agent fire suppression systems such as FM-200 and Inergen are recommended for server rooms because they suppress fires without damaging electronic equipment. Water, foam, and powder systems can destroy hardware and cause prolonged outages.
Clean agents extinguish fires by reducing heat or oxygen levels while remaining safe for occupied spaces.
NIST and data center best practices strongly recommend clean-agent systems for mission-critical environments.