Implementing Security Measures for Database Protection

Part 1: Office Roleplay Dialogue

Scenario: A Database Administrator, Sofia, is discussing security measures with her colleague, Ken, to protect sensitive data and prevent unauthorized access.

Ken: Hey Sofia, I heard that there was an attempted breach on one of our databases last week. What measures are we taking to improve security?

Sofia: We're strengthening our **encryption** protocols to ensure all sensitive data is securely stored and unreadable to unauthorized users.

Ken: That's a good step. Are we also reviewing our **access control** policies? We should make sure that only authorized employees can view or modify critical data.

Sofia: Yes, I've updated the **access control** list so that permissions are restricted based on **user roles**. Employees only get access to what they need.

Ken: That makes sense. What about **authentication**? Are we adding any extra security layers?

Sofia: Absolutely! We're implementing multi-factor **authentication** to verify user identities before they can log in.

Ken: Sounds like a solid plan. And how's our **firewall** setup? Is it blocking suspicious traffic?

Sofia: I checked the logs this morning. The **firewall** is working well, but I'll fine-tune the settings to prevent potential threats more effectively.

Ken: Good thinking. Security threats are always evolving, so we have to stay ahead of them.

Sofia: Exactly. I'll also schedule regular security audits to ensure our defenses remain strong.

Ken: That's a great idea! Let me know if you need any help running the audits.

Sofia: Will do! Thanks, Ken. The more proactive we are, the safer our data will be.

Part 2: Comprehension Questions

1. What is encryption used for?
(A) To make the database load faster
(B) To delete old files from the system
(C) To protect sensitive data by making it unreadable to unauthorized users
(D) To improve website design

2. How does access control help improve security?
(A) By restricting permissions based on user roles
(B) By allowing all employees to access all data
(C) By making the firewall stronger
(D) By increasing database storage

3. Why is authentication important for database security?
(A) It speeds up query processing
(B) It compresses large files for storage
(C) It removes duplicate records from the database
(D) It verifies user identities before granting access

4. What role does a firewall play in security?
(A) It increases internet speed
(B) It blocks unauthorized access and suspicious traffic
(C) It backs up all database records automatically
(D) It translates database queries into multiple languages

Part 3: Key Vocabulary Definitions in Japanese

1. **Encryption (暗号化)** – データを保護するために、情報を変換し第三者が読めないようにする技術。
2. **Access Control (アクセス制御)** – データやシステムへのアクセスを制限し、許可されたユーザーのみが操作できるようにするセキュリティ対策。
3. **Authentication (認証)** – ユーザーが正当なアクセス権を持っているかを確認するプロセス。
4. **User Roles (ユーザーロール)** – ユーザーに特定の権限やアクセスレベルを割り当てるシステム。

5. **Firewall (ファイアウォール)** – ネットワークへの不正アクセスを防ぐためのセキュリティシステム。

Part 4: Questions & Correct Answers

1. **What is encryption used for?**
   ✅ (C) To protect sensitive data by making it unreadable to unauthorized users
2. **How does access control help improve security?**
   ✅ (A) By restricting permissions based on user roles
3. **Why is authentication important for database security?**
   ✅ (D) It verifies user identities before granting access
4. **What role does a firewall play in security?**
   ✅ (B) It blocks unauthorized access and suspicious traffic