Monitoring Website Security & Preventing Vulnerabilities

Part 1: Office Roleplay Dialogue

Scenario: A Web Developer, Satoshi, is working with his colleague, Emily, to monitor website security and apply updates to prevent potential **vulnerabilities**.

Emily: Hey Satoshi, I just ran a security scan, and it looks like we need to update a **security patch** for the CMS.

Satoshi: Good catch. Keeping our system updated is crucial to preventing **vulnerabilities** that hackers might exploit.

Emily: Exactly. Also, have you checked the **SSL/TLS** certificates? If they expire, our website might not be secure for users.

Satoshi: I checked them earlier. The **SSL/TLS** certificate is valid, but we should set a reminder before it expires.

Emily: Good idea. What about our **firewall** settings? Are they blocking any suspicious traffic?

Satoshi: I reviewed the logs, and the **firewall** is doing its job. It blocked several unauthorized access attempts this week.

Emily: That's a relief! And I assume all sensitive data is protected with **encryption**?

Satoshi: Yes, we're using strong **encryption** methods to secure user data. Everything looks good for now, but we should continue monitoring regularly.

Emily: Agreed! Let's schedule another security check next week.

Satoshi: Sounds like a plan. Thanks, Emily!

Part 2: Comprehension Questions

1. Why is updating security patches important?

(A) To add new colors to the website

(B) To prevent vulnerabilities that hackers might exploit

(C) To speed up image loading times

(D) To make the website easier to navigate

2. What does an SSL/TLS certificate do?

(A) It improves website loading speed

(B) It removes duplicate pages from the website

(C) It changes the font of the website text

(D) It encrypts data to ensure secure communication

3. How does a firewall help protect a website?

(A) It blocks unauthorized access and suspicious traffic

(B) It adds animations to the homepage

(C) It improves customer service response time

(D) It optimizes search engine rankings

4. Why is encryption important for website security?

(A) It makes the website load faster

(B) It prevents the website from crashing

(C) It protects sensitive user data from unauthorized access

(D) It increases the number of website visitors

Part 3: Key Vocabulary Definitions in Japanese

1. **SSL/TLS (SSL/TLS 証明書) –** ウェブサイトの通信を暗号化し、データの安全性を確保するセキュリティ技術。
2. **Security Patch (セキュリティパッチ) –** ソフトウェアの脆弱性を修正し、攻撃を防ぐための更新プログラム。
3. **Vulnerability (脆弱性) –** ハッカーに悪用される可能性のあるシステムの弱点やセキュリティの欠陥。
4. **Firewall (ファイアウォール) –** 不正なアクセスや悪意のあるトラフィックをブロックするセキュリティシステム。
5. **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。

Part 4: Questions & Correct Answers

1. **Why is updating security patches important?**
   ✅ (B) To prevent vulnerabilities that hackers might exploit
2. **What does an SSL/TLS certificate do?**
   ✅ (D) It encrypts data to ensure secure communication
3. **How does a firewall help protect a website?**
   ✅ (A) It blocks unauthorized access and suspicious traffic
4. **Why is encryption important for website security?**
   ✅ (C) It protects sensitive user data from unauthorized access