実務に役立つ情報セキュリティの基礎

CompTIA Security+™

S+ ecurity問題集

現場でも役立つ知識が身に付く

合格に必要な全知識をわかりやすく解説

SY0-301対応

TAC

暗号化

Q 014

暗号化の説明として適切なのはどれですか。

- a. データを一定の規則で変換し、パスワードをかけること
- b. データを一定のリズムで再生すること
- c. データを一定の規則で変換し、通信途中の盗聴を防ぐこと
- d. データを一定の量をバッファしてから送信すること

A

正解は「データを一定の規則で変換し、通信途中の盗聴を防ぐこと」です。

C

データを一定の規則で変換し、他人には内容が理解できない情報にすることを「暗号化する」といいます。鍵を持っているユーザーだけが、復号してデータの内容を理解することができるため、鍵を持たない第三者による通信途中の盗聴を防ぐことができます。

例えば「abc」という文字列の場合、それぞれの文字をアルファベットの並びで2文字後ろにずらすと「cde」という文字列になります。暗号の変換ルールを知らない第三者は、簡単には元の文字列「abc」に戻せません。

IP上の音声通話では、データを一定量バッファしてから一定のリズムで再生することで、ジッタ（揺らぎ）を抑制できます。

Q 015

対称暗号方式の特徴はどれですか。

- a. 送信者の秘密鍵を用いて暗号化する
- b. データの送受信に同じ鍵を使用する
- c. データの送受信に異なる鍵を使用する
- d. 受信者の公開鍵を用いて暗号化する

A

正解は「データの送受信に同じ鍵を使用する」です。

b

暗号化には、対称暗号方式（共通鍵暗号）と非対称暗号方式（公開鍵暗号）の2つがあります。
対称暗号方式は、暗号化と復号に同じ鍵を利用し、暗号処理を高速に行うことができます。安全に暗号／復号を行うために、情報を伝えたい相手にあらかじめ共通に利用する鍵を渡しておく必要があります。
非対称暗号方式は、ユーザーごとに秘密鍵と公開鍵のペアを用意し、暗号化と復号に異なる鍵を使用します。