問040008解説

◆解答

設問　ａ　ウ　　ｂ　エ　　ｃ　イ　　ｄ　イ

◆解説

認証システムに関する問題である。

認証システムは次の手段を用いる。

①　チケットの発行を要求するチケットという認証データ

②　サーバへのアクセス許可を受けるチケットという認証データ

③　クライアントを識別する認証子

鍵データベースに登録されている鍵

①　チケット発行サーバの鍵 KEYT

②　各ＡＰサーバの鍵 KEYS

③　利用者の鍵 KEYC

セションに使用される鍵

①　Ｃ-Ｔ間のセション鍵 KEYCT

②　Ｃ-Ｓ間のセション鍵 KEYCS

新認証システムの構成と方式

①　クライアントＣは、認証サーバにチケットを要求するチケットを要求する。

②　チケット要求サーバは、利用者の鍵KEYCで暗号化した鍵KEYCTとチケット発行サーバの鍵KEYTで暗号化したTICKETCTを送信する。

③　クライアントＣは、TICKETCTとKEYCTで暗号化したAUTHC1、ＡＰサーバＳのIDSをＡＰサーバＳに送信する。

④　チケット発行サーバは、ＡＰサーバＳの鍵で暗号化されたTICKETCSとKEYCTで暗号化されたKEYCSをクライアントＣに送信する。

⑤　クライアントＣは、TICKETCSとKEYCSで暗号化したAUTHC2をＡＰサーバＳに送信し、アクセス許可を受ける。

クライアントがアクセス許可を受けるプロセス

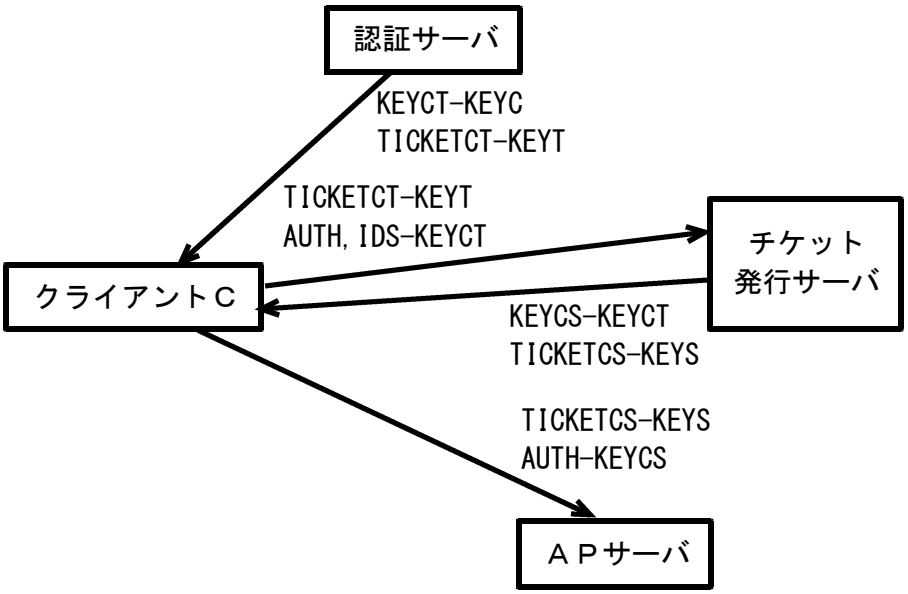
図中KEYCT-KEYCは、KEYCTがKEYCで暗号化されていることを示している。

KEYCTは、クライアントとチケット発行サーバ間のセション鍵を示している。

KEYCSは、クライアントとＡＰサーバ間のセション鍵を示している。

KEYTは、チケット発行サーバの鍵を示している。

KEYSは、ＡＰサーバの鍵を示している。



設問

ａは、チケットTICKETCTを暗号化するための鍵で、クライアントＣは復号する必要がないためチケット発行サーバの鍵で暗号化すればよい。KEYTで、求める答えはウとなる。

ｂは、クライアントＣとチケット発行サーバ間でAUTHやIDS、KEYCSを送信するための暗号化の鍵であるから、KEYCTとなり、求める答えはエとなる。

ｃは、チケットTICKETCSを暗号化するための鍵で、クライアントＣは復号する必要がないためＡＰサーバの鍵で暗号化すればよい。KEYSで、求める答えはイとなる。

ｄは、クライアントＣのAUTHを暗号がするための鍵であり、ＡＰサーバが復号できなければならないため、KEYCSの鍵を使用する。求める答えはイとなる。