問4　認証システム（情報セキュリティ）　(H22秋-FE 午後問4)

【解答】

［設問］　a－ウ，b－エ，c－イ，d－イ

【解説】

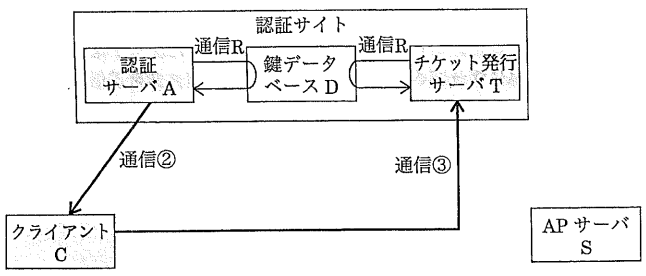
複数のアプリケーションサーバ（以下，APサーバという）が存在する環境で，サーバごとに異なるユーザID，パスワードを一度の認証で簡単に行う（シングルサインオン）ため，システムの認証からサーバリソースへのアクセスまでのロジックを考える問題である。空欄は四つだけであり一見簡単に見えるのだが，ロジックを確実に把握するためには問題文をよく読む必要がある。難易度としては普通といえる。

この問題の中で重要な点は，次の4点となる。

- 「認証サーバA」，「チケット発行サーバT」，「APサーバS」という三つのサーバと「クライアントC」が登場する点
- この三つのサーバはお互いの鍵を鍵データベースDを介して共有している点
- KEY_{CT}やKEY_{CS}は鍵データベースDを介して共有されていない点
- 「クライアントC」は「認証サーバA」からは「チケット発行サーバT」にアクセスするためのチケットを，「チケット発行サーバT」からは「APサーバS」にアクセスするためのチケットを受信する。

［設問］

・空欄a：通信②で認証サーバAから受信したデータを基にして，クライアントCがチケット発行サーバTに対して通信③としてデータを送信する場面が問題となっている。この場面は図Aのようになる。



図A　チケット発行サーバTへのアクセス

$enc(TICKET_{CT})$を暗号化するために必要な鍵を，どのコンピュータが知っているかを考えてみる。まず，共通鍵暗号方式で暗号化することから，少なくとも認証サーバAは知っている必要があることが分かる。次に，$enc(TICKET_{CT})$に格納されたデータがチケット発行サーバT向けのものであることから，チケット発行サーバTも鍵をもっている必要がある。最後にクライアントCであるが，問題文の通信③の説明のための表にある「$enc(TICKET_{CT})$」の説明を見ると，「$enc(TICKET_{CT})$は，クライアントCでは復号できない」とあるため，クライアントCはこの鍵を知らない。以上のことから，認証サーバA及びチケット発行サーバTしか知らない鍵が当てはまることが分かる。

ア，イ，エ：C-T間のセッション鍵KEY_{CT}，チケット発行サーバTのID ID_T，利用者ID ID_Cは，いずれもクライアントCが知っている情報であるため，間違いである。

したがって，（ウ）の「チケット発行サーバTの鍵KEY_T」が正解である。

・空欄b：通信③で暗号化される情報は$AUTH_{C1}$とID_Sである。これらの情報はクライアントCが最初に知っている情報であり，チケット発行サーバTに知らせたい情報である。このうちID_Sについては秘匿する必要性が明示されていないが，$AUTH_{C1}$は〔認証のための通信の例〕に「$TICKET_{CT}$を送信したのが間違いなくクライアントCであることを$TICKET_{CT}$と$AUTH_{C1}$から確認する」とあることから，漏えいしてしまうとクライアントCを偽装されてしまうので暗号化する必要があることが分かる。以上を踏まえると，ここで使用される鍵は，クライアントCとチケット発行サーバTだけが知っているものであることが分かる。したがって，（エ）の「C-T間のセッション鍵KEY_{CT}」が正解である。

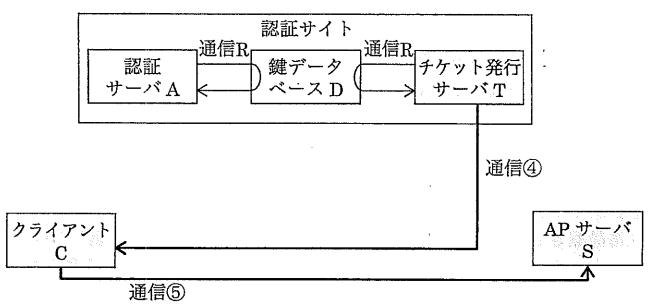
ア：APサーバSのID ID_Sをチケット発行サーバTが知るのは，通信③を受信して復号化した後であるため，通信③を受信した時点でチケット発行サーバTは，これを知らない。

イ：APサーバSの鍵KEY_Sは，クライアントCの知らない情報である。

ウ：C-S間のセッション鍵KEY_{CS}は，この時点ではどのコンピュータも知らない情報である。

オ：チケット発行サーバTの鍵KEY_Tは，クライアントCの知らない情報である。

・空欄c：通信④でチケット発行サーバTから受信したデータを基にして，クライアントCがAPサーバSに対して通信⑤としてデータを送信する場面が問題となっている。この場面は次の図Bになる。



図B　APサーバSへのアクセス

$enc(TICKET_{CS})$を暗号化するために必要な鍵は，$TICKET_{CS}$を生成するチケット発行サーバTと，APサーバSが知っている必要があることが分かる。問題文中の通信⑤の説明のための表にある，「$enc(TICKET_{CS})$」の説明を見ると，「$enc(TICKET_{CS})$は，クライアントCでは復号できない」とあるため，クライアントCはこの鍵を知らない。以上のことから，チケット発行サーバTとAPサーバSだけが知るものを選べばよいことが分かる。

ア：APサーバSのID ID_Sは，クライアントCが知っている情報である。

ウ：C-S間のセッション鍵KEY_{CS}は，クライアントCが知っている情報である。

エ：C-T間のセッション鍵KEY_{CT}は，クライアントCが知っている情報である。

オ：チケット発行サーバTの鍵KEY_Tは，APサーバSの知らない情報である。したがって，（イ）の「APサーバSのKEY_S」が正解である。

・空欄d：通信⑤でクライアントCがAPサーバSに対して$AUTH_{C2}$を送信する際に暗号化する理由は，送信者の正当性確認である（送信者のなりすまし防止である）と読み取れる。すなわち鍵としては，クライアントCとAPサーバSだけが知る情報を使う必要がある。したがって，（イ）の「C-S間のセッション鍵KEY_{CS}」が正解である。

ア：APサーバSの鍵KEY_Sは，クライアントCの知らない情報である。

ウ：C-T間のセッション鍵KEY_{CT}は，APサーバSの知らない情報である。

エ：チケット発行サーバTの鍵KEY_Tは，クライアントCの知らない情報である。