第３問　認証システムに関する次の記述中の空欄(a)～(e)に入れる正しい答えを、解答群の中から選べ。

複数のクライアントが複数のアプリケーションサーバを利用するネットワークにおいて、単純な認証システムを利用した場合には問題点が二つ考えられる。

①利用者は、クライアントPCからログインするAPサーバに対して、利用する都度ユーザIDとパスワードを入力しなければならない。

②クライアントPCとAPサーバの間の通信データの横取りと偽造によって、APサーバのサービスが不正に利用される危険性がある。

これらの問題点を解消するために次の認証サイトを使用した新たなシステムを構築することにした。

問題点①を解消するためにチケットを用いたシングルサインオンの仕組みを取り入れる。問題点②に対しては、APサーバに送信されたチケットが当該クライアントのものであることを確認できる認証子と呼ばれるデータを付与する。図１に認証の流れの例を、図２にそこでやりとりされるデータを示す。なお、この認証では共通鍵暗号方式を用いて通信データを暗号化する。それぞれの鍵は、クライアントＣ及び各サーバ自体と鍵データベースＤに登録されているものとする。

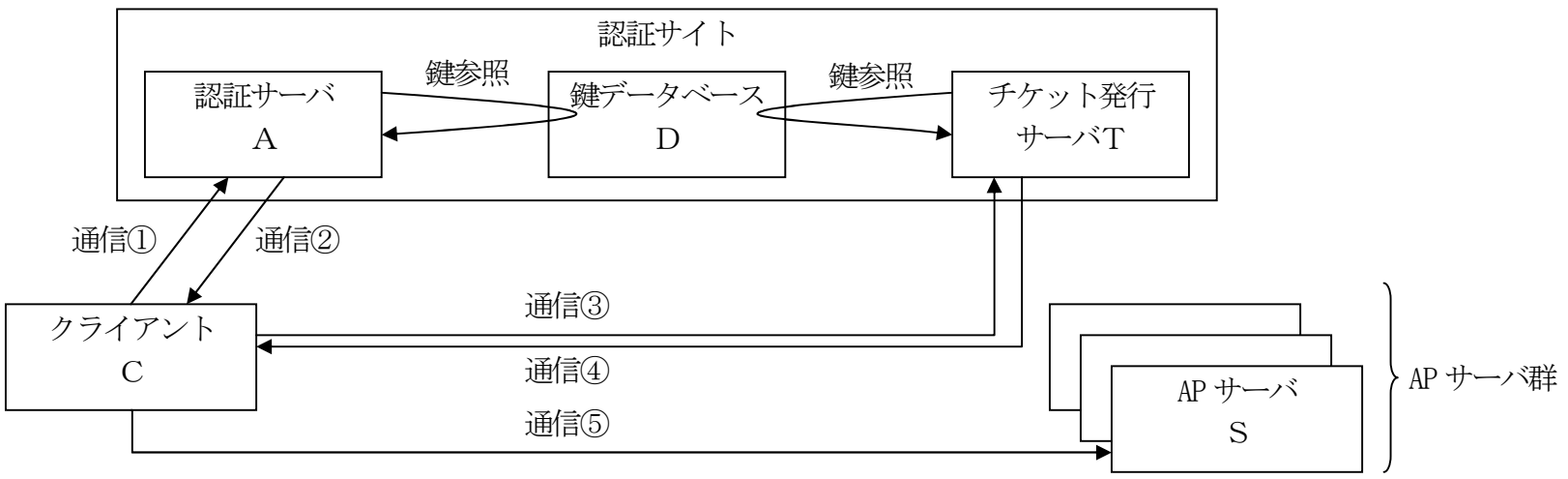
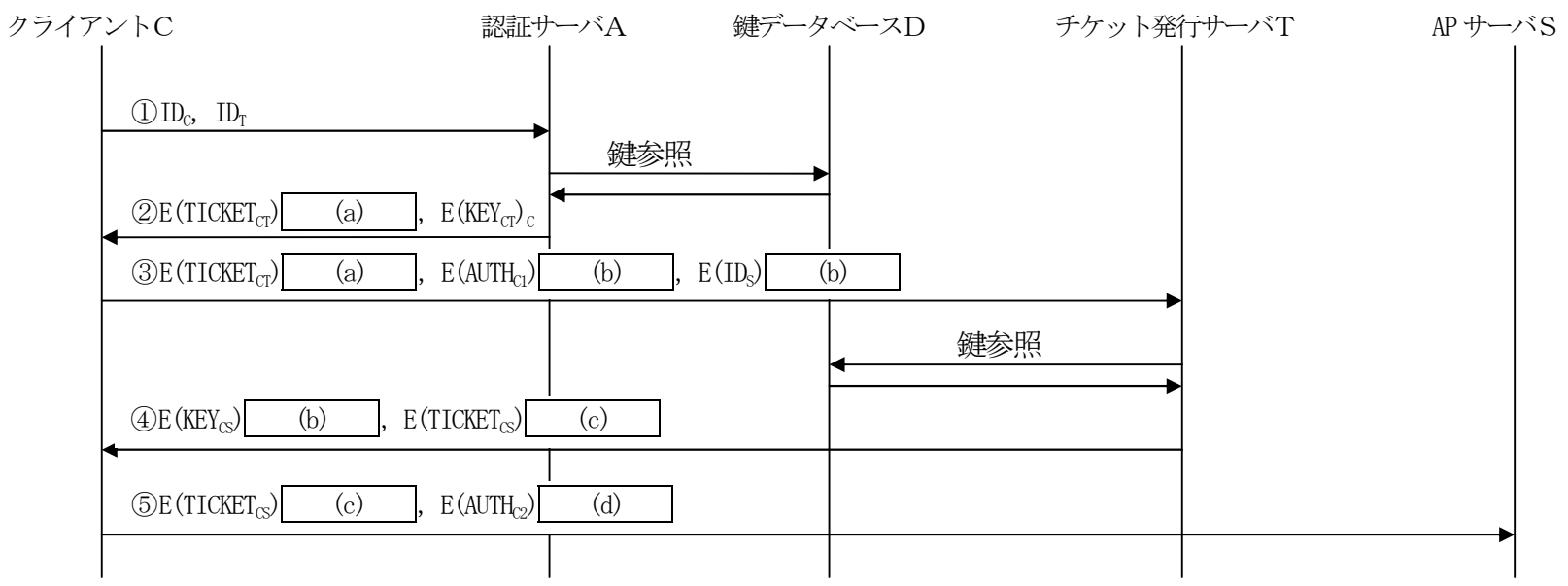


図１　認証の流れの例



注）ID_C, ID_T, ID_Sはそれぞれ、利用者ID、チケット発行サーバTのID、APサーバSのIDを表す。
　　E(　)xは括弧内のデータをKEYxで暗号化したものを表す。

図２　認証の際にやりとりされるデータの例

通信①　クライアントＣはチケット発行サーバＴにチケットを要求するためのチケットを取得するために、認証サーバＡに対してデータを送信する。

通信②　認証サーバＡはクライアントＣに応答する。KEY_{CT}はクライアントＣとチケット発行サーバＴとの間の通信データの暗号化に用いるセション鍵である。$TICKET_{CT}$はチケット発行サーバＴ用チケットであり、$TICKET_{CT}$はKEY_{CT}を含む。

通信③　クライアントＣがAPサーバＳ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に要求する。E($TICKET_{CT}$)はクライアントＣは復号できない。クライアントＣはチケット発行サーバＴにそのまま送信し、チケット発行サーバＴが復号する。また、認証子$AUTH_{C1}$はクライアントＣが生成する。

通信④　チケット発行サーバＴは、$TICKET_{CT}$と$AUTH_{C1}$を確認し間違いなく［　(e)　］ことを確認する。KEY_{CS}はクライアントＣとAPサーバＳとの間の通信データの暗号化に用いるセション鍵である。データの暗号化に用いた鍵は、チケット発行サーバＴが通信③で受け取ったデータから取り出したものである。$TICKET_{CS}$はAPサーバＳ用チケットであり、KEY_{CS}を含む。

通信⑤　APサーバＳ用のチケットを提示する。E($TICKET_{CS}$)はクライアントＣでは復号できない。クライアントＣはAPサーバＳにそのまま送信し、APサーバＳが復号する。また、$AUTH_{C2}$はクライアントＣが生成する。APサーバＳは$TICKET_{CS}$と$AUTH_{C2}$を確認し、間違いなく［　(e)　］ことを確認する。確認ができると、クライアントＣから、APサーバＳへのアクセスが許可される。

(a)～(d)に関する解答群

ア　C　　イ　T　　ウ　S　　エ　CT　　オ　CS

(e)に関する解答群

ア　認証サーバＡが送付した
イ　クライアントＣが送付した
ウ　チケット配信サーバＴが送付した
エ　APサーバＳが送付した