問4　認証システムに関する次の記述を読んで，設問に答えよ。

複数のクライアントと複数のアプリケーションサーバ（以下，APサーバという）が接続されているネットワークにおいて，単純な認証システムを利用する場合について，ここでは二つの問題点を取り上げる。

① 利用者は，使用するクライアントから各APサーバにログインするごとに，利用者IDとパスワードの入力操作を行わなければならない。

② クライアントとAPサーバと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。

ここで，これらの問題を改善するための認証システム（以下，新認証システムという）を考える。

なお，ここでは，これらの問題に直接関連しない仕様については，その記述を省略する。

〔新認証システムによる問題点の解消〕

問題点①に対しては，利用者が一度，利用者IDとパスワードをクライアントに入力して認証を受ければ，そのクライアントと各APサーバ間での認証は，利用者を介さないで済むように改善する。

このために，チケットと呼ぶ認証データを用いる。チケットは，クライアントに対して発行され，そのクライアントは，APサーバの認証を得るとき，発行されたチケットをAPサーバに送信する。

問題点②に対しては，APサーバに送信されたチケットが，チケットの発行を受けたクライアントから送られてきたものであることを，APサーバが確認できるよう，チケットとは別に認証子と呼ぶ認証データを用いる。

図1に新認証システムの構成を示す。

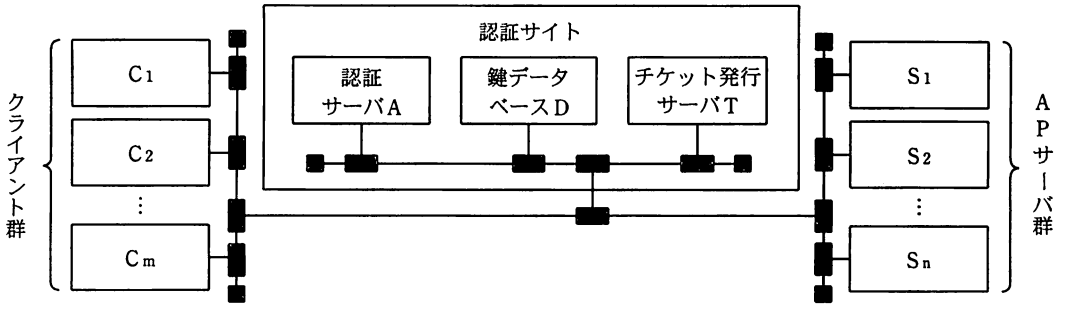


図1　新認証システムの構成

〔新認証システムの構成と方式についての説明〕

(1) 新認証システムでは，共通鍵暗号方式によって，通信データを暗号化する。以下，共通鍵を鍵という。

(2) 認証サイトは，認証サーバ，鍵データベース及びチケット発行サーバで構成する。

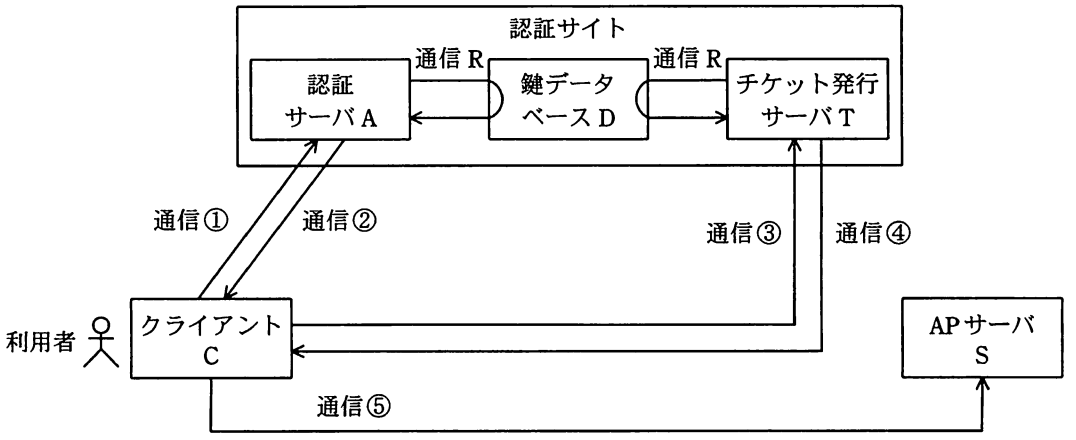
(3) チケット発行サーバの鍵は，チケット発行サーバ自体と鍵データベースに登録されている。

(4) 各 AP サーバの鍵は，それぞれの AP サーバ自体と鍵データベースに登録されている。

(5) 利用者の鍵は，利用者のパスワードから計算して決められ，鍵データベースに登録されている。クライアントには，利用者が入力したパスワードから計算した鍵が，利用者がクライアントの利用を終了するまで，一時的に保持される。

〔認証のための通信の例〕

図 2 は，利用者が，クライアント C から目的の AP サーバ S にアクセスする場合の認証の流れを示す。



注 通信 R は，鍵データベースを参照していることを表す。

図 2　認証の流れの例

認証は，次の3段階で行われる。ここで，enc(x)は，xを暗号化したものを表す。

第1段階は，クライアントCが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（以下，チケット発行サーバT用チケットという）の認証サーバAへの要求（図2中の通信①）と，その発行（図2中の通信②）である。

通信①では，クライアントCは，次のデータを認証サーバAに送信する。

データ	データの説明
ID_C	利用者IDである。
ID_T	チケット発行サーバTのIDである。

通信②では，認証サーバAは，次のデータをクライアントCに応答する。

データ	データの暗号化に用いた鍵	データの説明
$enc(KEY_{CT})$	利用者の鍵 KEY_C	KEY_{CT}は，クライアントCとチケット発行サーバTとの間（以下，C-T間という）の通信データの暗号化に用いる鍵であり，C-T間のセッション鍵という。
$enc(TICKET_{CT})$	a	$TICKET_{CT}$は，チケット発行サーバT用チケットである。$TICKET_{CT}$はKEY_{CT}を含む。これによって，チケット発行サーバTにクライアントC経由でKEY_{CT}を安全に渡すことができる。

第2段階は，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（以下，APサーバS用チケットという）のチケット発行サーバTへの要求（図2中の通信③）と，その発行（図2中の通信④）である。

通信③では，クライアントCは，次のデータをチケット発行サーバTに送信する。

データ	データの暗号化に用いた鍵	データの説明
$enc(TICKET_{CT})$	a	$enc(TICKET_{CT})$は，クライアントCでは復号できない。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。
$enc(AUTH_{C1})$	b	認証子$AUTH_{C1}$は，クライアントCが生成する。
$enc(ID_S)$	b	ID_Sは，APサーバSのIDである。

チケット発行サーバTは，$TICKET_{CT}$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。確認ができたとき，通信④では，チケット発行サーバTは，次のデータをクライアントCに応答する。

データ	データの暗号化に用いた鍵	データの説明
enc(KEY_{CS})	b	KEY_{CS}は，クライアントCとAPサーバSとの間（以下，C-S間という）の通信データの暗号化に用いる鍵であり，C-S 間のセッション鍵という。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 enc($TICKET_{CT}$)から取り出したものである。
enc($TICKET_{CS}$)	c	$TICKET_{CS}$は，APサーバS用チケットである。$TICKET_{CS}$は，KEY_{CS}を含む。これによって，APサーバSにKEY_{CS}をクライアントC経由で安全に渡すことができる。

第3段階は，APサーバS用チケットの提示である（図2中の通信⑤）。

通信⑤では，クライアントCは，次のデータをAPサーバSに送信する。

データ	データの暗号化に用いた鍵	データの説明
enc($TICKET_{CS}$)	c	enc($TICKET_{CS}$)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。
enc($AUTH_{C2}$)	d	認証子$AUTH_{C2}$は，クライアントCが生成する。

APサーバSは，$TICKET_{CS}$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$TICKET_{CS}$と$AUTH_{C2}$から確認する。確認ができたとき，利用者は，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。

設問　本文中の［　　］に入れる正しい答えを，解答群の中から選べ。

aに関する解答群

ア　C-T間のセッション鍵 KEY_{CT}　　イ　チケット発行サーバTのID ID_T

ウ　チケット発行サーバTの鍵 KEY_T　　エ　利用者ID ID_C

b，cに関する解答群

ア　APサーバSのID ID_S　　イ　APサーバSの鍵 KEY_S

ウ　C-S間のセッション鍵 KEY_{CS}　　エ　C-T間のセッション鍵 KEY_{CT}

オ　チケット発行サーバTの鍵 KEY_T

dに関する解答群

ア　APサーバSの鍵 KEY_S　　イ　C-S間のセッション鍵 KEY_{CS}

ウ　C-T間のセッション鍵 KEY_{CT}　　エ　チケット発行サーバTの鍵 KEY_T