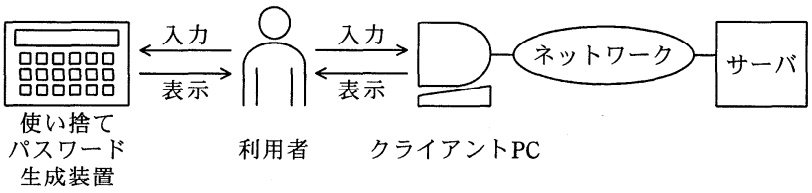
問040002問題

サーバへのログイン管理に関する次の記述を読んで，設問に答えよ。

使い捨てパスワード(One-Time Password:OTP)の仕組みを応用して作られた，ログイン管理システムである。



〔ログイン管理システムの説明〕

サーバへのログイン可能回数Ｍと定数Ｋを決定し，Ｍ個の有効な使い捨てパスワードを使用する。残りのログイン可能回数がｎのときの使い捨てパスワードotp(n)には，一方向性関数hashを用いて，次式で得られる値を用いる。

$$otp(n) = \overbrace{hash(hash(\cdots hash(K)\cdots))}^{n\text{回}}$$

（１）使い捨てパスワード生成装置

利用者が，使い捨てパスワードをすべて記憶し，管理することは困難なので，定数Ｋと残りのログイン可能回数ｎから使い捨てパスワードを生成し，表示する携帯式の使い捨てパスワード生成装置を用いる。

第１回目のパスワード生成時はｎ＝Ｍで，パスワードを生成するたびにｎを１ずつ減らし，最後のパスワード生成時は，ｎ＝１となる。

（２）利用者

利用者は，Ｋを使い捨てパスワード生成装置に入力し，表示された使い捨てパスワードを，サーバへのログインパスワードとしてクライアントＰＣに入力する。

（３）サーバ

サーバは，次の二つを保持する。

① 使い捨てパスワード生成装置と同じ一方向性関数hash

② パスワード検査に用いるために，利用者が，直前の許可されたログインで使ったパスワードotp(n+1)

サーバでのパスワード検査は，ログイン時にクライアントＰＣからサーバへ送られてきた使い捨てパスワードotp(n)に，hashを１回適用し，hash(otp(n))を得て，それがサーバの保持しているotp(n+1)と一致するかどうかで行う。一致すれば，サーバは，ログインを許可する。

サーバは，保持しているotp(n+1)を次回の検査用に更新する必要がある。このためには，クライアントＰＣから送られてきた使い捨てパスワードの値otp(n)で置き換えればよい。

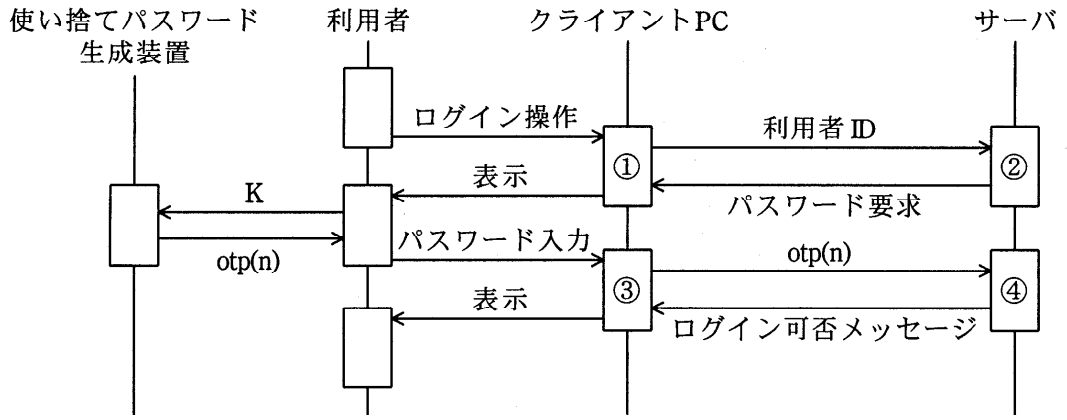


図　ログイン管理の流れ

図にログイン管理の流れを示す。ここでは，サーバには，利用者のotp(n)を受け入れる準備として，otp(n+1)が保持されているものとする。また，この図では，時間は上から下に向かって進むように表現されている。

〔図中の主な処理の説明〕

① 利用者ＩＤによってサーバにログイン操作を行う。

② パスワードを要求する。

③ 使い捨てパスワードotp(n)をサーバへ送る。

④ 受け取ったotp(n)にhashを適用し，hash(otp(n))を得る。利用者ＩＤごとに保存していたotp(n+1)と比較する。一致すれば，ログインを許可し，受け取ったotp(n)を次回のパスワード検査用に保持する。一致しなければ，ログインを拒否する。

設問 このログイン管理に関する次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

利用者がパスワードとしてクライアントＰＣに入力する［　ａ　］は，ネットワーク上の通信メッセージにも含まれる。しかし，［　ａ　］は，ログイン許可と同時に無効なパスワードとなるので，これを盗聴してその後で使用しても，サーバにログインすることはできない。

サーバが保持する使い捨てパスワードotp(n+1)は，使用済みの無効なパスワードなので，これを不正に入手して使用しても，サーバにログインすることはできない。

また，otp(n+1)とhashを不正に入手したとしても，hashの一方向性の特徴から，これらを基に，未使用の使い捨てパスワードを得ることは極めて困難である。

このログイン管理の仕組みで，不正アクセスの危険性が大きいのは，［　ｂ　］と［　ｃ　］の両方が不正に入手，使用された場合である。

このうち，［　ｂ　］は，サーバと使い捨てパスワード生成装置にある。サーバには，セキュリティ強化のための既存の手段を講じることができるが，使い捨てパスワード生成装置は，別の利用者も所有しているので，その不正使用及び盗難の危険性は比較的高い。

［　ｃ　］は，クライアントＰＣ，ネットワーク上の通信メッセージ及びサーバには一時的にも存在しない情報なので，これらから盗まれる危険性はない。また，［　ｃ　］は，利用者本人だけが知る秘密情報である。

解答群

ア　hash	イ　Ｋ	ウ　Ｍ	エ　ｎ
オ　otp(M+1)	カ　otp(n)	キ　利用者ＩＤ	