

## 問040007問題

利用者認証に関する次の記述を読んで、設問1、2に答えよ。

X社では、社外の端末から社内のサーバへのリモートログインを可能にするため、利用者認証の方式を検討している。社内では、利用者IDとパスワードをサーバに送信する方式を使用しており、そのパスワードの強化を含め、次の三つの方式の安全性を検討している。

〔方式1：利用者IDとパスワード方式〕

端末は、利用者が入力した利用者IDとパスワードをサーバに送信する。サーバは利用者IDから登録されているパスワードを検索し、送信されたパスワードと照合することによって、ログインの可否を応答する。利用者IDとパスワード方式を図1に示す。

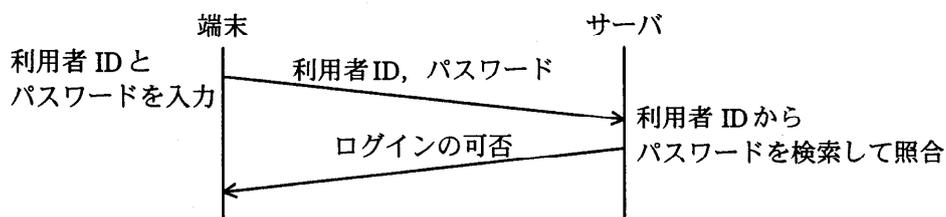


図1 利用者IDとパスワード方式

〔方式2：チャレンジレスポンス方式〕

端末は、利用者が入力した利用者IDをサーバに送信する。サーバは、利用者IDを受信すると、ランダムに生成したチャレンジと呼ばれる値  $c$  を端末に送信する。端末は、利用者が入力したパスワード  $p$  とチャレンジ  $c$  から、ハッシュ値  $h(p, c)$  を計算して、レスポンスの値としてサーバに送信する。サーバは、利用者IDから登録されているパスワード  $p'$  を検索し、端末と同じハッシュ関数  $h$  を使って計算したハッシュ値  $h(p', c)$  とレスポンスの値とを照合することによって、ログインの可否を応答する。ここで、ハッシュ関数  $h$  は公知のものであり、どの端末でも計算可能とする。チャレンジレスポンス方式を図2に示す。

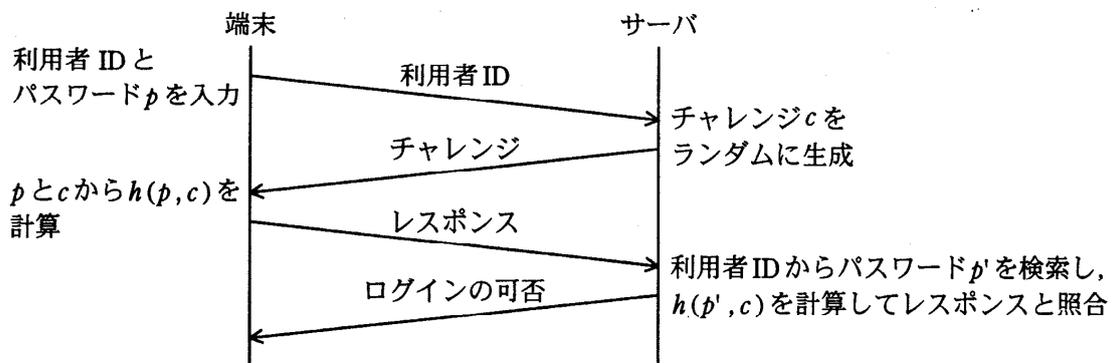


図2 チャレンジレスポンス方式

〔方式3：トークン(パスワード生成器)方式〕

利用者には、自身の利用者IDが登録されたトークンと呼ばれるパスワード生成器を配布しておく。トークンの例を図3に示す。

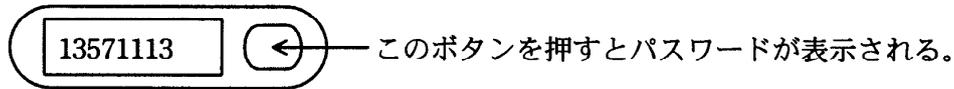


図3 トークンの例

トークンは時計を内蔵しており、関数  $g$  を使らて、利用者IDである  $u$  と時刻  $t$  に応じたパスワード  $g(u, t)$  を生成し表示することができる。利用者は、利用者IDとトークンが生成し表示したパスワードを入力し、端末はこれらをサーバに送信する。サーバは、利用者IDである  $u$  とサーバの時刻  $t$  からトークンと同じ関数  $g$  を使って生成したパスワード  $g(u, t)$  と端末から受信したパスワードとを照合することによって、ログインの可否を応答する。

なお、トークンの時刻とサーバの時刻が同期していることは保証されており、トークンのパスワード表示からサーバにおけるパスワード生成までの遅延も、一定の時間は許容する。トークン方式を図4に示す。

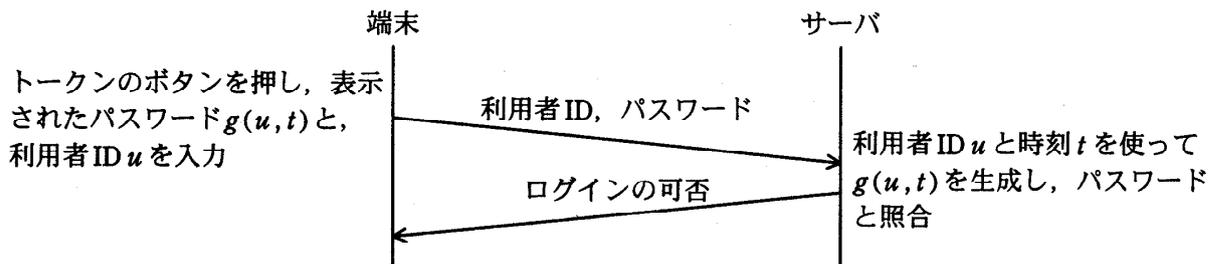


図4 トークン方式

**設問1** パスワードの強度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。

方式1, 2では、利用者がパスワードを設定する。これらの方式を採用する場合には、容易には推定されないパスワード、すなわち、十分な強度をもつパスワードを、利用者に設定してもらう必要がある。

パスワードの強度を高めるためには、パスワードを長くすることやパスワードに利用する文字の種類を増やすことが考えられる。例えば、英小文字26文字だけからなる8文字のパスワードに対して、総当たり方式による発見に必要な最大時間を1とすると、パスワードの長さを10文字にすれば必要な最大時間は  a  となる。また、同じ8文字であっても、英大文字も使用する場合、必要な最大時間は  b  となる。

