問040002解説

◆解答

設問　ａ　カ　　ｂ　ア　　ｃ　イ

◆解説

使い捨てパスワードを使用してサーバにログインする仕組みの問題である。

ワンタイムパスワード(使い捨てパスワード)

ワンタイムパスワードとは、遠隔地にある端末からネットワークを通じてサーバコンピュータを利用する(リモートアクセス)際に、アクセスしてくる人間が正規のユーザかどうかを検証する認証技術のひとつである。

ユーザ名と対応するパスワードを送信する通常の認証方式では、端末からサーバまでの通信経路上でパスワードが「盗み聞き」されてしまう可能性があるという弱点がある。ＯＴＰでは、まずサーバが端末に認証文字列の「種」となるランダムな文字列(「チャレンジ」と呼ばれる)を送信する。ユーザは自分しか知らない秘密のパスワードを端末に入力する。端末に備えられたソフトウェアがサーバから送られてきたチャレンジ文字列とユーザが入力したパスワードを一定の手順に従って演算し、生成された結果(「レスポンス」と呼ばれる)をサーバに送信する。サーバでは受け取った文字列を検証し、正規のユーザかどうかを調べる。

チャレンジは毎回異なる文字列になるように設定されており、ユーザが申告したパスワードも毎回異なった文字列としてサーバに送信される。このため、万が一通信経路上でサーバと端末のやり取りを盗み聞きされても、同じパスワードは二度と使えないため、サーバが不正使用されることはない。

使い捨てパスワードの作成方法

① 定数Ｋ、ログイン可能回数Ｍを使用して、使い捨てパスワードを作成する。
② 残りのログイン可能回数をｎとすると、定数ＫとHash関数を用いて、Ｋをｎ回Hashして、使い捨てパスワードを求める。
③ 利用者は、定数Ｋをパスワード生成装置に入力して、Hash関数を用いて求めた表示される使い捨てパスワードを使用する。
④ 使い捨てパスワードを使用すると、次の使い捨てパスワードは、定数Ｋをｎ－１回Hashして使い捨てパスワードを求めることができる。
⑤ 最後の使い捨てパスワードは、定数Ｋを１回Hashして求める。
⑥ パスワードの検証は、入力された使い捨てパスワードをサーバで１回Hashして、前回に使用したパスワードと一致すれば、ログインが許可される。
⑦ 入力された使い捨てパスワードは、次回のパスワード検証用に保持される。
⑧ 毎回入力される使い捨てパスワードが変化し、基準値も変化する。

設問

ａは、利用者がクライアントＰＣに入力するパスワードで、残りの使用回数がｎの場合、定数Ｋをｎ回hashして求めたopt(n)であり、求める答えはカとなる。

ｂは、使い捨てパスワードの作成に関係する要素は定数Ｋとhash関数の内容である。この２つか不正に使用されると、使い捨てパスワードが生成できることになる。このうち、パスワード生成装置とサーバにはhash関数が格納されており、サーバはセキュリティ対策で不正使用を防止することができるが、パスワード生成装置は不正使用の危険性が高くなる。答えはhashで、求める答えはアとなる。

ｃは、もう一つの要素で、定数Ｋである。Ｋは利用者本人だけが知る情報で、パスワード生成装置に利用者が入力することによって使用する。クライアントＰＣ、ネットワーク上のメッセージ、サーバには存在しない情報である。答えは定数Ｋで、求める答えはイとなる。