1 次の文章を読み，下の問いに答えよ。(100点)

コンピュータシステムやインターネット上のサービスを利用する際，あらかじめ登録した正規の利用者であることを確認するために［（ア）］を行う。［（ア）］では，ユーザIDによって利用者を［（イ）］する。しかし，誰でも①そのユーザIDを名乗ることができてしまうため，利用者は本人であることを証明する必要がある。一般的には，本人だけが知る文字列のパスワードを用いる。ユーザIDとパスワードの組み合わせがあらかじめ登録されたものと一致していれば，そのユーザIDを登録した本人であると認められる。最近では，人間の身体の固有の特徴値から読み取った照合データを用いる生体認証(あるいは［（ウ）］)や，②信用できる第三者が発行した［（エ）］を用いる電子認証も利用されるようになってきたが，現状ではパスワードの利用が主流である。

パスワードを決める際には，他人が［（オ）］しやすいものを避け，英文字の大文字・小文字，数字，記号を混ぜて短すぎないようにしなければならない。しかし，利用しようとしているインターネット上のサービスが，登録できるパスワードに例えば「0～9の数字4桁」等の制限を設けていることもありうる。そのようなサービスの利用は避けたほうがよい。なぜなら，そのようなサービスは逆総当たり攻撃を防ぐことが難しいからである。通常の総当たり攻撃は［（A）］を繰り返す手法であり，この攻撃を防ぐには，誤ったパスワードの試行が連続して何度も繰り返された場合にそのユーザIDの使用を一定時間禁止にする対策を行えばよい。しかし，逆総当たり攻撃は［（B）］を繰り返すため，この対策方法が無効になってしまう。逆総当たり攻撃をされにくくするには，登録できるパスワードのパターン数を増やさなくてはならない。もしパスワードがサービスによって「0～9の数字4桁」と制限された場合，パスワードのパターン数は［（C）］である。このサービスの利用者が1000万人いたとして単純計算すると，1つのパスワードあたりの利用者は平均で［（D）］人もいることになり，根気よく試行を繰り返せば平均でそれだけの利用者のパスワードが判明してしまうことになる。パスワードに使用できる文字の種類に数字だけでなく英文字の大文字・小文字(A，B，…，Z，a，b，…，z)も含めるようにすれば，パスワードの長さが［（E）］以上でパターン数が1000万を超え，さらに文字数制限をなくせばパターン数は無限大となるため，逆総当たり攻撃は現実的ではなくなる。ただし当然ながら，登録できるパスワードのパターン数を増やしても，③利用者が安易なパスワードを設定してしまうと逆総当たり攻撃を受けるリスクは高まってしまう。

学習指導要領（4）- 知・技 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

問 1 （ア） ～ （オ） の空欄に入る適切な語を以下より選択せよ。

アプライアンス　許諾　サーバ証明　識別　電子証明書　同意
バイオメトリクス　プロトコル　URL　ユーザ認証　類推

学習指導要領（1）- 知・技 - イ
学習内容（1）- イ 法・情報セキュリティ・情報モラル

問 2 下線①に書かれたことを不正に行うことを何というか，以下より選択せよ。

改ざん　情報漏洩　盗聴　なりすまし　フィッシング

学習指導要領（1）- 知・技 - イ
学習指導要領（4）- 知・技 - ア
学習内容（1）- イ 法・情報セキュリティ・情報モラル
学習内容（4）- ア ネットワークの仕組みと構成要素

問 3 下線②で示した電子認証は，暗号化と復号化とで異なる鍵を用いる暗号方式に基づいている。この暗号方式を何というか，以下より選択せよ。

共通鍵暗号方式　公開鍵暗号方式　シーザー暗号方式
対称鍵暗号方式　秘密鍵暗号方式　ブロック暗号方式

学習指導要領（1）- 知・技 - イ
学習指導要領（1）- 思・判・表 - イ
学習内容（1）- イ 法・情報セキュリティ・情報モラル

問 4 （A） と （B） に入る文を以下より選択し，それぞれ番号で答えよ。

1．同一のユーザ ID とパスワードを様々なサービスへ試行
2．同一のユーザ ID に対して様々なパスワードの試行
3．同一のパスワードに対して様々なユーザ ID の試行
4．同一のサービスに対して故意に大量の接続要求の送信

学習指導要領（1）- 知・技 - イ
学習指導要領（1）- 思・判・表 - イ
学習内容（1）- イ 法・情報セキュリティ・情報モラル

問 5 （C） と （D） と （E） に入る数字をそれぞれ答えよ。

学習指導要領（1）- 思・判・表 - イ
学習内容（1）- イ 法・情報セキュリティ・情報モラル

問 6 下線③の理由を 100 字以下で説明せよ。