次の問1は必須問題です。必ず解答してください。

問1　ソーシャルネットワーキングサービスのセキュリティに関する次の記述を読んで，設問1～3に答えよ。

P社は，ソーシャルネットワーキングサービスの運営会社である。P社のサービス（以下，P-SNSという）は，約30,000人の会員が利用している。PCやスマートフォンのWebブラウザから簡単に日記や写真を登録できることが人気で，会員数を伸ばしつつある。

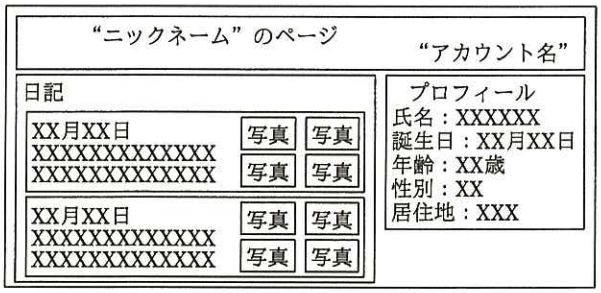
〔P-SNSの利用方法〕

P-SNSの利用には，会員登録が必要である。利用を希望するユーザは，会員情報として希望するアカウント名とパスワード，電子メールアドレス，ニックネーム，プロフィール情報（氏名，誕生日，年齢，性別，居住地）を入力し会員登録を行う。会員登録をすると，P-SNS内にマイページが作成される。

会員登録後は，アカウント名とパスワードを用いてP-SNSにログインし，日記や写真を登録して，マイページを更新する。

P-SNSでは，マイページ内の日記や写真について，情報の公開範囲の設定が可能であり，P-SNS内に無制限に公開するか，特定の会員だけに公開するかを設定できる。ただし，日記や写真以外の情報については，公開範囲の設定ができず，P-SNS内に無制限に公開される。

日記と写真をP-SNS内に無制限に公開する設定にした場合，他の会員がPCのWebブラウザからアクセスしたときに見える P-SNSのマイページのイメージを図1に示す。



注記　“ニックネーム”と“アカウント名”は，会員登録時に入力したニックネームとアカウント名に置き換えられる。

図1　P-SNSのマイページのイメージ

〔P-SNS のアカウント名とパスワードの設定ポリシ〕

P-SNS では，アカウント名とパスワードの設定ポリシを図 2 のように定めており，設定ポリシを満たさないアカウント名やパスワードは設定できないように，会員登録時やパスワード変更時に入力チェックが行われる。

アカウント名の設定ポリシ
・アカウント名長は，6 文字以上 32 文字以下
・利用可能な文字は，半角英数字
・他の会員と重複したアカウント名の設定は不可
パスワードの設定ポリシ
・パスワード長は，6 文字以上 32 文字以下
・利用可能な文字は，半角英数字，記号文字
・英大文字，英小文字，数字のうち少なくとも 2 種を組み合わせた文字列

図 2　アカウント名とパスワードの設定ポリシ

〔不正ログインの発覚〕

ある日，会員の Q さんから P 社に，“情報の公開範囲の設定が勝手に変更され，日記や写真が無制限に公開されている”とのクレームが入った。

そこで，P 社カスタマサポート担当の R 君が，Q さんのアカウントの利用状況調査を行うことになった。まず，R 君がアクセスログからログイン状況を調査したところ，クレームの前日に，Q さんのアカウントでログインを試みるアクセスが 100 回あったことを確認した。そのうち，99 回はパスワード誤りによってログインが拒否されており，最後の 1 回でログインが成功していた。また，Q さんへのヒアリングから，Q さん自身はこの日にログインしていないことが分かった。そこで，R 君は，Q さんのアカウントが第三者による不正ログインに使用されたと判断し，Q さんのアカウントの利用を停止し，P-SNS の全会員に不正ログインの事件発生について注意喚起の案内を行った。

次に R 君は，Q さんへのヒアリングから，設定されていたパスワードが氏名と誕生日を組み合わせた単純なものであったことが判明したので，今回の攻撃は［ a ］である可能性が高いと判断した。また，アカウント名とパスワードの組合せが第三者に知られたことから，［ b ］に備えて，P-SNS と同じパスワードを設定している他のサービスについてもパスワードを変更するように，Q さんにアドバイスした。

〔不正ログインに対する調査〕

R 君は，Q さん以外の会員のアカウントに対する不正ログインについても調査を行った。その結果，Q さんの場合と同様の 100 回程度のログイン試行の記録が幾つか見つかった。

R 君は，P-SNS のマイページには，①公開範囲の設定ができない情報の中にこれらの攻撃の足掛かりとなるものがあり，不正ログインにつながるリスクが高いと考えた。

〔不正ログイン対策の検討〕

R 君は，不正ログイン対策として，次の三つの対策を検討した。

対策 1 ：アカウント名とパスワードの設定ポリシを見直して，悪意をもった第三者が P-SNS に不正ログインしにくくする。

対策 2 ：パスワード誤りによってログインが一定の回数拒否された場合，アカウントの利用を自動的に停止する機能を追加する。

対策 3 ：悪意をもった第三者が P-SNS に不正ログインできないように，アカウント名とパスワードによる認証に加え，Cookie による認証を追加する。

対策 3 を採用した場合の，会員登録から初回ログインまでの手順を図 3 に示す。

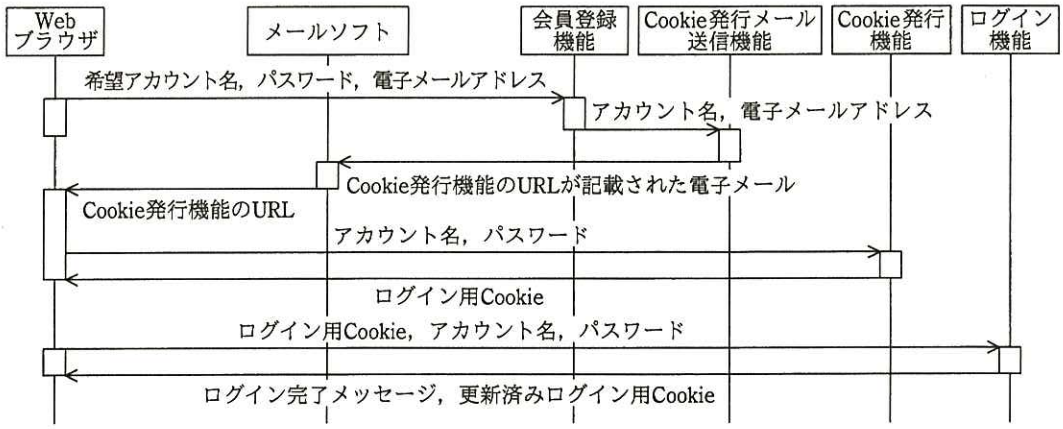


図 3　対策 3 を採用した場合の会員登録から初回ログインまでの手順

ユーザが Web ブラウザを用いて会員登録機能から会員登録を行うと，Cookie 発行機能の URL が記載された電子メール（以下，メールという）が Cookie 発行メール送

信機能から送信される。ユーザは，メールソフトを用いてメールを受信し，メール内に記載された URL から Cookie 発行機能に Web ブラウザを用いてアクセスする。ユーザがアカウント名とパスワードを入力し認証が完了すると，ログイン用 Cookie が発行される。Cookie 発行機能の URL は，登録した会員一人一人にメールを送信する都度，異なるものが発行され，メールの送信から 1 時間だけ有効である。また，発行されたログイン用 Cookie の有効期間は半年間とし，ログインするたびに有効期間がその日から半年間に更新される。

会員が P-SNS にログインするときには，会員が入力するアカウント名とパスワードとともにログイン用 Cookie がログイン機能へ送信される。ログイン機能では，送信されたログイン用 Cookie がその会員に発行されたログイン用 Cookie と異なる場合にはアクセスを拒否する。

会員が利用端末を変更したい場合や Cookie の有効期間が過ぎた場合には，Cookie 発行メール送信機能に対して，Cookie 発行機能の URL が記載されたメールの送信を要求する。その後，会員登録時と同様にログイン用 Cookie を入手する。

なお，P-SNS の通信は暗号化し，悪意をもった第三者が盗聴しても必要な情報を入手できないようにする。

その後 R 君は，アカウントへの不正ログインの足掛かりとなった情報を全会員のマイページから削除するとともに，Cookie による認証機能の導入を行った。

設問 1　本文中の［ a ］，［ b ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

a に関する解答群

ア　DoS 攻撃　　イ　サイドチャネル攻撃

ウ　標的型攻撃　　エ　類推攻撃

b に関する解答群

ア　ゼロデイ攻撃　　イ　総当たり攻撃

ウ　パスワードリスト攻撃　　エ　フィッシング攻撃

設問 2　本文中の下線①について，攻撃の足掛かりとなる情報とは何か。プロフィール情報とニックネームを除く情報の中から，10 字以内で答えよ。

設問3　〔不正ログイン対策の検討〕について，(1)～(4)に答えよ。

(1) 対策 1 について，Q さんのアカウントへの攻撃手法に対する対策として有効ではないものを，解答群の中から選び，記号で答えよ。

解答群

ア　英和辞典にある英単語の利用禁止

イ　パスワード中に会員情報として登録した文字列を含めることの禁止

ウ　パスワードに記号文字を含めることの必須化

エ　半年以上ログイン実績がないアカウントの利用停止

(2) アカウント名とパスワードによる認証がユーザを認証するのに対し，Cookie による認証は何を認証するものか。10 字以内で答えよ。

(3) 図 3 の手順によって，今回のような悪意をもった第三者のログインが拒否される理由を 25 字以内で述べよ。

(4) 図 3 の手順を用いることで，会員登録時に入力した情報の有効性を確認できる。どの情報の有効性を確認できるか。15 字以内で答えよ。