問1　認証システムの開発に関する次の記述を読んで，設問1～4に答えよ。

S社は，従業員10名のベンチャー企業である。S社のファイル共有サービス（以下，Sサービスという）は機能が豊富であり，登録会員（以下，S会員という）の数を伸ばしている。

Sサービスでは，利用者認証されたS会員が写真などのファイルを自身に割り当てられたフォルダにアップロードできる。さらに，当該ファイルにアクセスするためのURLを電子メールなどで他者に示すことによって，当該ファイルを他者と共有できる。また，Sサービス内でメッセージや“いいね”を送信できる。

Sサービスの企画，開発及び運用は，CTOのF氏が取り仕切っており，そのうち，開発と運用は，F氏の指示の下，S社エンジニア2名が行っている。Sサービスは，外部セキュリティ企業による脆弱性診断を随時受けている。

〔Sサービスの改修〕

前回の脆弱性診断では，利用者IDとパスワードを用いて利用者認証するSサービスの認証モジュール（以下，S認証モジュールという）の認証方式を，多要素認証にする方がよいとのアドバイスを受けたが，その対処が課題であった。そこで，F氏は，認証及び認可を提供するSNS（以下，認証認可提供SNSという）のうち，多要素認証などの機能をもつT社のTサービスとSサービスとをID連携する改修をCEOのX氏に提案した。その改修によって，S認証モジュールを用いないS会員の登録と多要素認証の実現を目指す。ただし，今回の改修でのID連携では，既存のS会員は対象とせず，新規登録のS会員だけを対象とする。改修後も当面は既存のS会員の認証のために，S認証モジュールも継続して稼働させる。

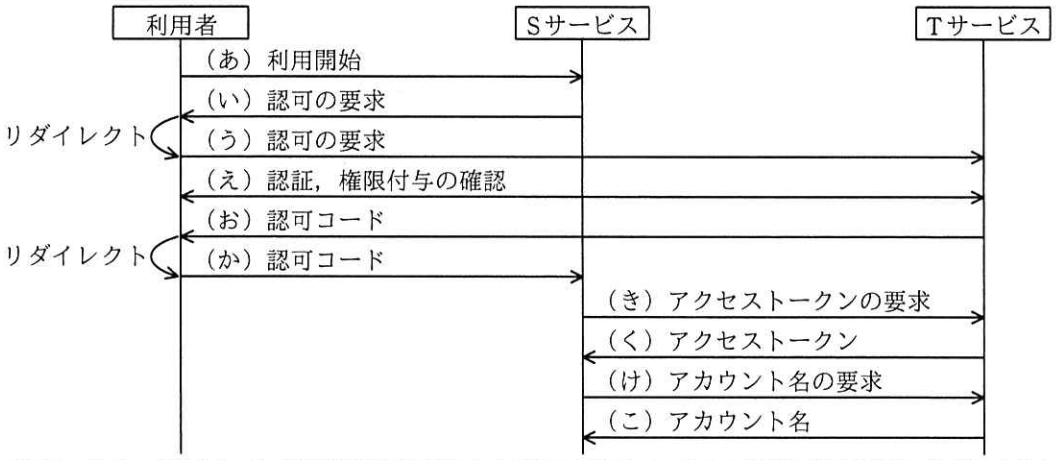
F氏は，①S認証モジュールの代わりにTサービスとのID連携を利用することにはどのような利点と欠点があるかをX氏に説明した。X氏は，ID連携技術に詳しい情報処理安全確保支援士（登録セキスペ）のY氏を外部から招聘して，実装の最終段階でのレビューを受けることを前提に，Sサービスの改修を承認した。

今回の改修では，OAuthのAuthorization Code Grantを採用する。OAuthは，認証認可提供SNSと認可情報を送受信するためのプロトコルの一つである。OAuthを用いた認可における三つの主体の説明を図1に，認可のシーケンスを図2に示す。

利用者	：T サービスのアカウントをもち，S 会員の登録を希望する者（以下，S 会員登録希望者という）及び登録された S 会員である。
S サービス	：T サービスでのアカウント名を要求する。
T サービス	：認証認可提供 SNS である。図 3 に示す権限を提供する。

注記　T サービスのアカウント名は変更できない。

図 1　OAuth を用いた認可における三つの主体の説明



注記　S サービスは，S 会員登録希望者による利用の初回に，S 会員登録希望者がログイン中の T サービスから取得したアカウント名（以下，T-ID という）を S サービス内に登録する。T サービスにログインしていない場合はログインが促される。2 回目以降の S サービスの利用の場合，初回に登録された T-ID を確認する。

図 2　OAuth を用いた認可のシーケンス

（ア）　他の利用者の投稿に対し“いいね”を送信する権限
（イ）　他の利用者へのメッセージを送信する権限
（ウ）　利用者の代わりに投稿する権限
（エ）　利用者のアカウント名，電子メールアドレスなど登録情報を取得する権限

図 3　T サービスが提供する権限

図 2 のシーケンスにおいて，［ a ］は，［ b ］が提供するリソースにアクセスできる。それは［ c ］が，図3に示す権限を［ a ］に与えるからである。［ c ］は［ a ］に与える権限を図 2 中の［ α ］の通信の際に確認する。図 3 のうち，どの権限を要求するかは，［ a ］の実装者が決定する。S 社では，要求した権限のいずれか一つでも，［ c ］が与えることを拒否する場合は，シーケンスを止めるように実装することにした。

なお，S サービスでは，将来どの権限も利用すると考え，図 3 の全権限を要求する

ことにした。

次に，T サービスと S サービスとの ID 連携について，実装の最終段階で Y 氏のレビューを受けた。Y 氏はセキュリティ上の問題を三つ指摘した。

〔一つ目の問題〕

Y 氏は，一つ目の問題を，次の攻撃シナリオで説明した。

S サービスにログインしていない利用者が攻撃者の用意した罠(わな)サイトにアクセスすると，図 4 中に示すシーケンス X が走り，後に，②利用者が攻撃を受けているとは知らずに S サービスにファイルをアップロードすると，そのファイルを攻撃者にダウンロードされてしまうおそれがある。

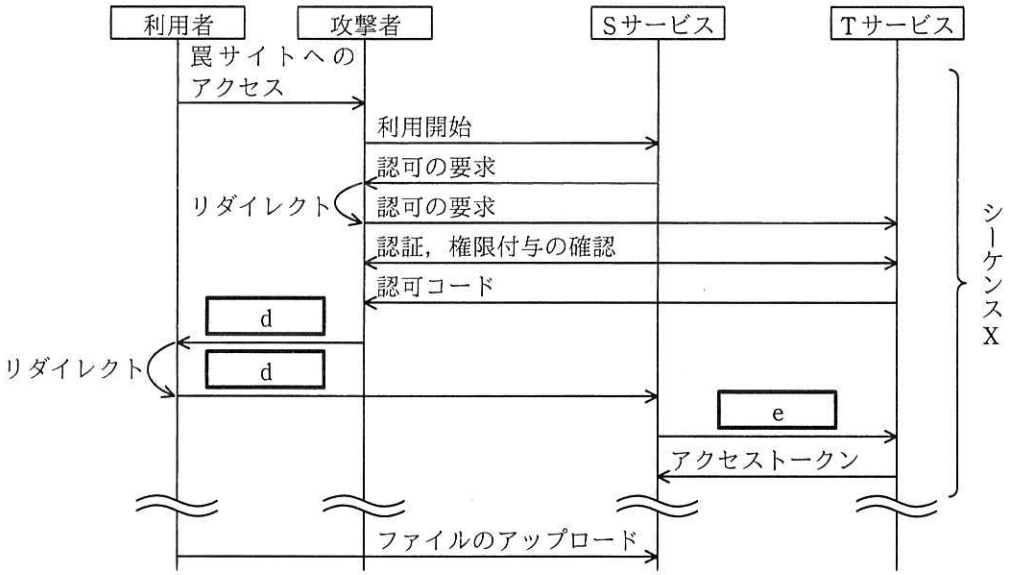


図 4　攻撃のシーケンス

この対策として，RFC 6749 は，図 2 のシーケンスで，推測困難な値である state パラメタを利用することを推奨している。S サービスは state パラメタを［ β ］を送信する際に付与する。S サービスは［ γ ］を受信する際に，そのセッションが，state パラメタを付与した際の［ β ］のセッションと同一であるか否かを確認する。同一である場合だけシーケンスを続ける。

〔二つ目と三つ目の問題〕

二つ目の問題は，③S サービスが T サービスに要求する権限が必要最小限のものになっていないことである。この問題については，要求する権限を一つだけにした。

三つ目の問題は，T サービスに深刻な脆弱性が報告された場合の対応方法を決めていなかったことである。この問題については，T サービスとの ID 連携を一時的に停止し，S 認証モジュールだけで認証することにした。ただし，このとき④一部の S 会員は S サービスを利用できなくなるので，対象の S 会員向けに代替策を検討することにした。

〔利用者認証の実現について〕

X 氏は，全面改修して S 認証モジュールを停止した後の利用者認証の実現方式について Y 氏に確認した。S サービスは利用者を直接認証していないが，⑤S サービスは，登録された S 会員をどのように利用者認証しているかを，Y 氏は X 氏に解説した。

S 社では，Y 氏から指摘された問題を解決した後，T サービスと S サービスとの ID 連携を開始した。

設問 1　〔S サービスの改修〕について，(1)～(4)に答えよ。

(1) 本文中の下線①について，S 社の課題に即した利点を 30 字以内で具体的に述べよ。

(2) 本文中の下線①について，可用性の観点での欠点を 30 字以内で述べよ。

(3) 本文中の［ a ］～［ c ］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。

解答群

ア　S サービス　　イ　T サービス　　ウ　利用者

(4) 本文中の［ α ］に入れる適切な字句を，図 2 中の（あ）～（こ）から選び，記号で答えよ。

設問2　〔一つ目の問題〕について，(1)～(3)に答えよ。

(1) 図4中の［　d　］，［　e　］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。

解答群

ア　アクセストークンの要求　　イ　アクセストークン

ウ　認可コード　　エ　認可の要求

オ　認証，権限付与の確認

(2) 本文中の下線②について，ファイルのアップロードと，ファイルのダウンロードは，それぞれTサービスの誰のアカウントによって行われるか。それぞれ6字以内で答えよ。

(3) 本文中の［　β　］，［　γ　］に入れる適切な字句を，図2中の（あ）～（こ）から選び，記号で答えよ。

設問3　〔二つ目と三つ目の問題〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，必要最小限の権限を図3中の（ア）～（エ）から一つ選び，記号で答えよ。

(2) 本文中の下線④に該当するS会員を，35字以内で述べよ。

設問4　本文中の下線⑤について，Sサービスは，Tサービスと連携して，どのように利用者認証を実現しているか。実現の方法を50字以内で具体的に述べよ。