問3　クラウドサービスの認証連携に関する次の記述を読んで，設問1～3に答えよ。

F社は，従業員数300名のソフトウェア開発会社である。F社では，社外のクラウドサービスを試行的に導入し始めており，交通費精算サービス，グループウェアサービス，オンラインストレージサービスの三つを現在利用している。これらのクラウドサービスには，各クラウドサービスの利用者IDとパスワードを用いてログインする。これらのクラウドサービスは，社内からの利用に限定するという社内ルールを定めている。

従業員が利用する端末は，社内ネットワークに設置されており，ウイルス対策ソフトが導入され，最新のウイルス定義ファイルが毎日適用されている。社外から社内ネットワークへの通信はファイアウォールによって禁止されている。端末からクラウドサービスを利用する際には，プロキシサーバを経由する必要がある。

〔クラウドサービスへの不正アクセス〕

ある日，交通費精算サービスで従業員の振込先口座が勝手に変更されたとの相談が，経理部から情報システム部のC主任にあった。Rさんの振込先口座がF社指定の銀行以外の口座に変更されていたので，Rさんに確認したところ，本人による変更ではないことが分かったとのことであった。

C主任は，社外の攻撃者による不正アクセスの可能性を考え，交通費精算サービスに記録されているログイン記録を調査した。F社で利用しているクラウドサービスではログイン記録として，アクセス日時，利用者ID，接続元IPアドレス，接続先URLが記録されている。調査の結果，Rさんの利用者IDによるログイン記録には，接続元IPアドレスとして，F社のIPアドレス以外に，海外のIPアドレスが一つあった。Rさんに話を聞いたところ，このログインには心当たりがないということであった。Rさんに更に詳しく話を聞いたところ，4月9日に交通費精算サービスから登録情報の確認を促す電子メール（以下，メールという）が1通，Rさんの私用メールアドレスに届いており，Rさんが4月10日にそのメールを自宅で読み，記載内容に従って自宅からログイン操作を行ったことが分かった。そのメールをRさんから転送してもらい，C主任がメールに記載されていたURLを確認したところ，交通費精算サービスを模したフィッシングサイトであった。C主任はこのフィッシングサイト

から利用者 ID とパスワードが盗まれた可能性が高いと判断した。そこで，R さんがパスワードを使い回している可能性も考慮して，他のクラウドサービスに対する R さんのログイン記録も調査した。その結果，他のクラウドサービスに対する R さんの利用者 ID を用いたログインは，F 社からのものだけであることを確認した。

今回は金銭的な損害に至らなかったが，情報システム部の B 部長は早急な対策が必要と考え，C 主任に暫定対策の実施と根本的な対策の検討を指示した。

〔暫定対策の実施と根本的な対策の検討〕

C 主任はまず，暫定対策として三つの対策を行うことにした。第一に，フィッシングメールに注意するよう従業員に周知した。第二に，F 社で利用している各クラウドサービスに対するログイン記録を C 主任が調査して，①F 社以外からのログインがあった利用者 ID を特定し，その利用者 ID を利用する者にはパスワードを変更させることにした。第三に，F 社以外からのログインを検知できるよう，ログイン記録の監視を行うことにした。C 主任は暫定対策が完了したことを確認し，根本的な対策の検討を開始した。

C 主任は，今回の不正アクセスの原因の一つが，F 社の IP アドレス以外からクラウドサービスへのログインが可能になっていたことにあると考え，F 社の IP アドレス以外からのログインを制限することが可能か調査した。F 社で利用しているクラウドサービスのうち，グループウェアサービスだけは，接続元 IP アドレスを制限する機能を備えていたので，その機能を有効化し，社内からだけログインできるように設定した。しかし，残りのクラウドサービスは接続元 IP アドレスの制限機能を備えていなかった。

C 主任は，接続元を制限する他の方法を検討した。その結果，クラウドサービスへログインする際，F 社に既に設置してある LDAP サーバでの認証を必要とすることにすれば，接続元を制限できるようになると考えた。そこで，F 社で利用しているクラウドサービスを調べたところ，全て SAML（Security Assertion Markup Language）を用いた認証連携に対応していることが分かった。C 主任は，クラウドサービスと LDAP サーバとの間で，SAML を用いた認証連携による接続元の制限を検討することにした。

〔SAML を用いた認証連携と接続元制限方式の概要〕

SAML は，認証，認可などの情報を安全に交換するためのフレームワークである。SAML を用いることによって，利用者にサービスを提供するサービスプロバイダ（以下，SP という）と，ID プロバイダ（以下，IdP という）との間で利用者の認証結果などの情報を安全に連携することができる。SAML には複数の処理方式が存在する。今回 F 社で導入を検討している方式のシーケンスを図 1 に示す。図 1 中の各通信のプロトコルは，IdP と LDAP サーバ間は LDAP であり，それ以外は HTTP over TLS である。

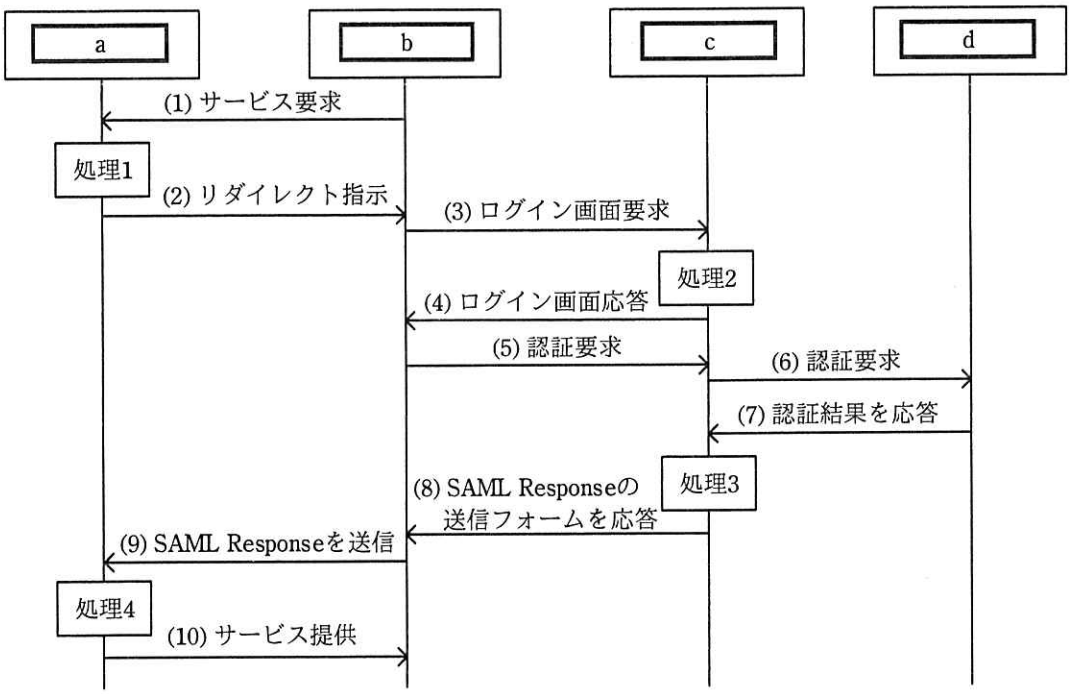

図 1　導入を検討している方式のシーケンス

SAML を用いた認証連携を行うためには，事前に IdP と SP との間で様々な情報を共有することによって，信頼関係を構築しておく必要がある。事前に共有する情報としては，通信の方式や連携する属性情報などが記述されたメタデータ，［　e　］で生成して送出する URL，［　f　］において必要な IdP のディジタル証明書などがある。

図 1 中の処理 1～4 の処理内容を表 1 に示す。

表1　処理内容

処理番号	処理内容
処理1	・IdPに認証を要求するSAML Requestを生成する。 ・SAML Requestをエンコードする。 ・エンコード結果をIdPのログイン画面のURLと組み合わせて，リダイレクト先URLを生成する。
処理2	・URL内の［　g　］からSAML Requestを取得する。 ・信頼関係が構築されたSPからの認証要求であることを検証する。
処理3	・利用者の認証が成功した場合，認証結果やSPとの間で連携する属性情報，有効期間，それらの情報に対するディジタル署名を含めたSAML Responseを生成する。
処理4	・SAML Responseに含まれるディジタル署名を検証することによって，ディジタル署名が［　h　］によって署名されたものであること，及びデータの［　i　］がないことを確認する。 ・SAML Response内の属性情報も検証することによって，サービスを提供すべきか決定する。

C主任は図1のシーケンスから，②IdPを社内ネットワークに設置しても認証情報の連携が成立することを確認した。そこで，IdPは社内ネットワークに設置し，IdPのログイン画面のURLのFQDNには，社内のFQDNを割り当てることにした。

〔SAMLを用いた認証連携と接続元制限の動作検証〕

最後にC主任は，F社で利用しているクラウドサービスを用いて，SAMLによる認証連携の動作を検証することにした。C主任はIdPを社内ネットワークに設置して必要な設定を行い，各クラウドサービス上に，既に利用しているものとは別の検証用アカウントを作成し，社内からのクラウドサービスへのログインが可能であることを確認した。また，③社外からクラウドサービスへのログインを試みると，失敗することも確認した。

C主任は検証結果をB部長に説明し，承認を得て，SAMLを用いた認証連携と接続元制限を開始した。また，シングルサインオンも併せて実現したことによって，クラウドサービスを利用する従業員の利便性も向上させることができた。

設問1　本文中の下線①について，条件を満たす利用者 ID を特定するためには，どのような条件を満たすログイン記録を抽出すればよいか。満たすべき条件を 35 字以内で述べよ。

設問2　〔SAML を用いた認証連携と接続元制限方式の概要〕について，(1)～(5)に答えよ。

(1) 図 1 中の［ a ］～［ d ］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 IdP　　イ LDAP サーバ

ウ SP　　エ 利用者端末の Web ブラウザ

(2) 本文中の［ e ］，［ f ］に入れる適切な処理番号を，表 1 中の処理 1～4 の中から選び，答えよ。

(3) 表 1 中の［ g ］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 Cookie　　イ HTML　　ウ クエリ文字列

エ スキーム　　オ リファラ

(4) 表 1 中の［ h ］，［ i ］に入れる適切な字句を，それぞれ 5 字以内で答えよ。

(5) 本文中の下線②について，SP と IdP が直接通信できないにもかかわらず，認証情報の連携が成立するのはなぜか。その理由を，35 字以内で述べよ。

設問3　本文中の下線③について，社外から交通費精算サービスとグループウェアサービスにアクセスしたとき，それぞれのサービスは，異なる理由でログインに失敗する。それらは，図 1 中のどの通信ができないことによるものか。図 1 中の(1)～(10)から選び，答えよ。また，その理由を，それぞれ 35 字以内で述べよ。