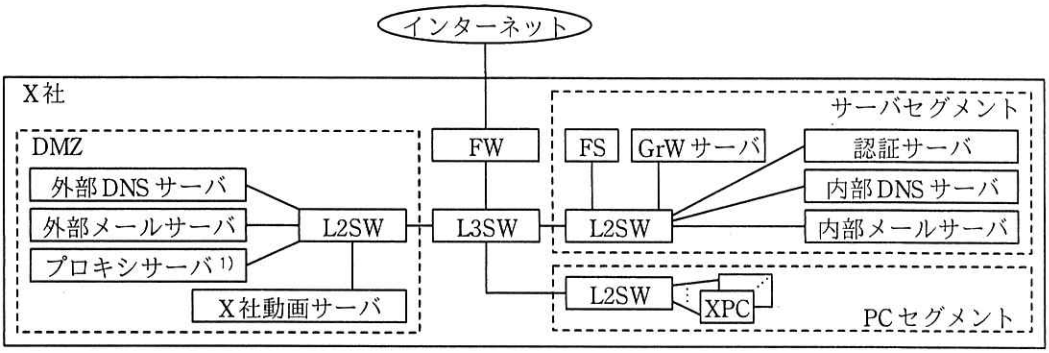
問2　クラウドサービスへの移行に関する次の記述を読んで，設問1～5に答えよ。

X社は，従業員500名の情報サービス会社であり，5年前から動画投稿配信サービス（以下，動画サービスという）を提供している。動画サービスは，アカウント登録した会員が動画を投稿したり，投稿された動画を閲覧して評価したりすることができるサービスである。動画サービスは，Webサーバ（以下，動画サービスを提供するWebサーバをX社動画サーバという）を用いて提供されている。X社のシステム部は，X社のシステム全てを管理している。X社のシステム構成を図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　GrW：グループウェア
FS：ファイルサーバ　L3SW：レイヤ3スイッチ　XPC：会社貸与の業務PC
注1)　拒否リストに登録したFQDNを宛先とする通信を遮断する機能がある。

図1　X社のシステム構成

XPCには，Webブラウザ，電子メール（以下，メールという）ソフト，GrW用クライアントソフトなどが導入されている。X社の従業員の認証は，認証サーバで行われており，XPC，GrWサーバ，FS，内部メールサーバへのシングルサインオン（以下，シングルサインオンをSSOという）を実現している。

X社のシステムでは，動画サービスの人気上昇による会員の増加に伴い，X社動画サーバの負荷が高くなっており，インターネット回線もひっ迫している。

X社の経営陣は，この問題への対策と併せて，セキュリティを強化するための抜本的な対策を検討するようシステム部に指示した。システム部のCさんが担当に指名され，セキュリティサービスを提供するW社から情報処理安全確保支援士（登録セキスペ）のF氏を招き，助言を受けることになった。

〔抜本的な対策の検討〕

F 氏は，X 社動画サーバをクラウドサービスへ移行し，さらに，Content Delivery Network（CDN）を利用する案を図 2 のように提案した。

1　X 社動画サーバのクラウドサービスへの移行 コンピュータリソースを柔軟に増強できるようにするため，X 社動画サーバをクラウドサービス事業者の IaaS に移行する。クラウドサービス事業者が提供する FW 及び IPS の利用を検討する。 2　CDN の利用 X 社動画サーバの可用性を高めるため，CDN を利用する。CDN の利用によって，セキュリティ対策の効果も期待できる。

図 2　X 社動画サーバのクラウドサービスへの移行及び CDN の利用案（抜粋）

次は，図 2 の 2 についての C さんと F 氏の会話である。

C さん：X 社動画サーバでの動画配信に CDN を利用すると，どのように動画が配信されるようになりますか。

F 氏　：CDN では，インターネット上に［　a　］サーバというサーバを分散配置して，動画配信を要求した端末に最も近い［　a　］サーバから動画を配信するようにします。［　a　］サーバは，動画配信を要求されたとき，要求された動画を保持していれば代理応答し，保持していなければ動画を保持している X 社動画サーバにアクセスして動画を取得し，応答します。多くの動画配信が代理応答されるので，X 社動画サーバの負荷が軽減されます。

C さん：その仕組みによって，［　b　］攻撃への耐性も向上しますね。X 社動画サーバでの動画配信に CDN を利用するには，どのようにすればよいでしょうか。

F 氏　：例えば，M 社が提供している CDN を採用した場合の利用手順は図 3 のようになり，動画配信時の動作は図 4 のようになります。

(1)　M 社 CDN から X 社動画サーバ用に割り当てられた FQDN（以下，X-CDN-M-FQDN という）が発行される。 (2)　X 社の外部 DNS サーバの CNAME レコードで，X 社動画サーバの FQDN（以下，X-FQDN という）と X-CDN-M-FQDN とをひも付ける。

図 3　M 社 CDN の利用手順（抜粋）

(1) 会員が端末から X 社動画サーバに動画配信を要求すると，X 社の外部 DNS サーバに問合せが届く。X 社の外部 DNS サーバは，図 3 の設定に基づいて，X-CDN-M-FQDN を返す。
(2) 会員の端末は，M 社の DNS サーバに問い合わせて，X-CDN-M-FQDN の名前解決を行う。
(3) 会員の端末は，X-CDN-M-FQDN を名前解決した IP アドレスのサーバとの HTTPS 通信を行うため，TLS 接続を確立する。
(4) 会員の端末は，動画配信を要求する HTTP リクエストを送信する。TLS の接続先サーバ名には RFC 6066 に基づいて，HTTP リクエストの [c] ヘッダには RFC 7230 に基づいて，X-FQDN が指定される。要求された動画を M 社 CDN が保持していない場合，M 社 CDN は，HTTP リクエストの [c] ヘッダから X 社動画サーバを特定し，HTTP リクエストを転送する。

図 4　動画配信時の動作（抜粋）

C さん：理解しました。CDN を悪用する攻撃というのはあるのでしょうか。

F 氏　：X 社動画サーバの CDN 利用に関するものではありませんが，CDN を悪用する攻撃の一つにドメインフロンティング攻撃があります。X 社内のインターネット利用者を FW とプロキシサーバで保護するセキュリティ対策では，注意が必要です。どのようにして攻撃が成功するか，その例を図 5 に示します。

(1) ある CDN（以下，CDN-U という）が，X 社内から頻繁にアクセスする他社の Web サイトの複数で利用されているとする。それらの Web サイトの一つを Y 社 Web サイトとする（以下，Y 社 Web サイトの FQDN を Y-FQDN といい，CDN-U から Y 社 Web サイト用に割り当てられた FQDN を Y-CDN-U-FQDN という）。また，CDN-U は攻撃者サーバも利用しているとする（以下，攻撃者サーバの FQDN を Z-FQDN といい，CDN-U から攻撃者サーバ用に割り当てられた FQDN を Z-CDN-U-FQDN という）。
(2) この状況で XPC の 1 台がマルウェアに感染すると，次のような攻撃が行われることがある。
(3) 当該マルウェアは，Y 社 Web サイトとの HTTPS 通信を行うため，Y-FQDN の名前解決を行うと，まず Y-CDN-U-FQDN が返される。次に，Y-CDN-U-FQDN の名前解決を行い，Y-CDN-U-FQDN を名前解決した IP アドレスのサーバとの HTTPS 通信を行うため，TLS 接続を確立する。
(4) 当該マルウェアは，HTTP リクエストを送信する際，[c] ヘッダに Z-FQDN を指定する。CDN-U は，攻撃者サーバに HTTP リクエストを転送することになる。
(5) 結果として，当該マルウェアと攻撃者サーバとの間の通信が CDN 経由でできてしまう。

図 5　ドメインフロンティング攻撃が成功する例

C さん：何か対策はあるのでしょうか。

F 氏　：攻撃者サーバに割り当てられた IP アドレスを宛先とする通信を FW で拒否しても，Z-FQDN をプロキシサーバの拒否リストに登録しても，図 5 の(5)の

通信は遮断できません。①Y-CDN-U-FQDN を名前解決した IP アドレスを宛先とする通信を FW で拒否すると，複数の Web サイトが閲覧できなくなる影響があります。通信内容を監視して遮断するなどセキュリティ強化を進めている CDN 事業者もありますが，進めていない事業者もあります。X 社では，FW 又はプロキシサーバを，アウトバウンド通信の復号及び高機能な通信解析ができるものに替え，[d] と HTTP リクエスト中の [c] ヘッダの値が一致していることを検証して，一致していなければ遮断するという対策を検討してもよいでしょう。

C さん：分かりました。

システム部は，X 社動画サーバのクラウドサービスへの移行及び CDN の利用案について経営陣に報告した。この案は経営陣に承認され，X 社動画サーバの移行が開始された。

〔他のサーバのクラウドサービスへの移行案〕

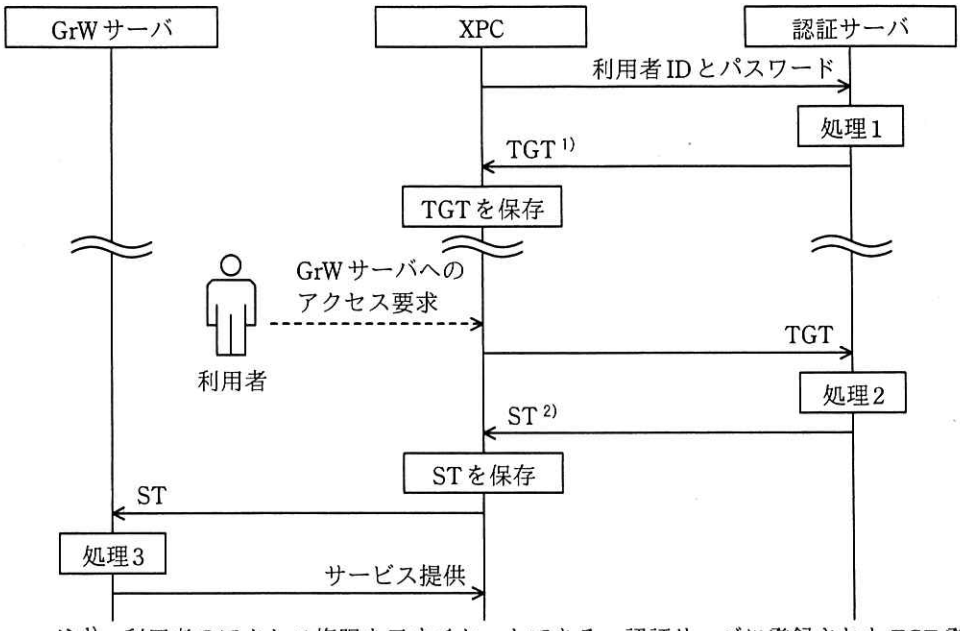
X社動画サーバの移行が完了し，CDNの利用も開始された。X社動画サーバに関する課題が解決されると，経営陣は，自社が保有する他のサーバについてもクラウドサービスへの移行を検討するようシステム部に指示した。システム部では，図 6 に示すクラウドサービスへの移行案を作成した。

・GrW 及びメールを SaaS に移行する。SaaS に切り替え後，GrW サーバ，外部メールサーバ及び内部メールサーバは，廃止する。 ・従業員の利便性を確保するために，移行後の SaaS でも SSO を実現する。

図 6　他のサーバのクラウドサービスへの移行案（抜粋）

〔SSO の現状〕

X 社では，Kerberos 認証で SSO が実現されている。XPC から GrW サーバにアクセスする場合の Kerberos 認証の流れを図 7 に，図 7 中の各処理の概要を表 1 に示す。



注 1) 利用者のアクセス権限を示すチケットである。認証サーバに登録されたTGT発行用アカウントのパスワードハッシュ値を鍵として暗号化されている。

注 2) アクセス対象のサーバごとに発行されるチケットである。アクセス対象のサーバの管理者アカウント（以下，サーバ管理者アカウントという）のパスワードハッシュ値を鍵として暗号化されている。

図7　XPCからGrWサーバにアクセスする場合のKerberos認証の流れ

表1　図7中の各処理の概要

処理名	処理内容
処理1	利用者IDとパスワードが正しければ，TGTを発行する。
処理2	TGTを復号して検証し，問題なければ，STを発行する。
処理3	STを復号して検証し，問題なければ，アクセスを許可する。

次は，図7についてのCさんとF氏の会話である。

Cさん：Kerberos認証に対する攻撃はあるのでしょうか。

F氏　：幾つかあります。二つ説明しましょう。一つ目は，TGT，ST の偽造攻撃です。TGT又はSTが偽造されると，サーバが不正アクセスされて危険です。現在，TGT の偽造については，認証サーバ側での対策が進んでいます。一方，②STの偽造については，認証サーバ側で検知することができません。

Cさん：リスクがありますね。

F氏　：二つ目は，サーバ管理者アカウントのパスワードを解読して不正にログインする攻撃です。XPCからSTが奪取され，不正アクセスに悪用されても，不正アクセスされる範囲は限定されます。しかし，奪取されたSTに対してサーバ管理者アカウントのパスワードの総当たり攻撃が行われ，それが成功すると，当該サーバ管理者アカウントでアクセスできるサーバが乗っ取られてしまいます。この総当たり攻撃は，③サーバ側でログイン連続失敗時のアカウントロックを有効にしていても対策になりません。

Cさん：分かりました。

〔SaaSでのSSOの実現〕

Cさんは，GrW及びメールのSaaSへの移行後のSSOの実現方法をF氏に尋ねた。次は，その際のF氏とCさんの会話である。

F氏　：IDaaSの利用を提案します。多くのIDaaSでは，Kerberos認証ではなくSAML認証をサポートしています。SaaS側がSAML認証をサポートしていれば，SAML認証を用いたSSOが可能です。SAML認証の流れを図8に，図8中の各処理の概要を表2に示します。

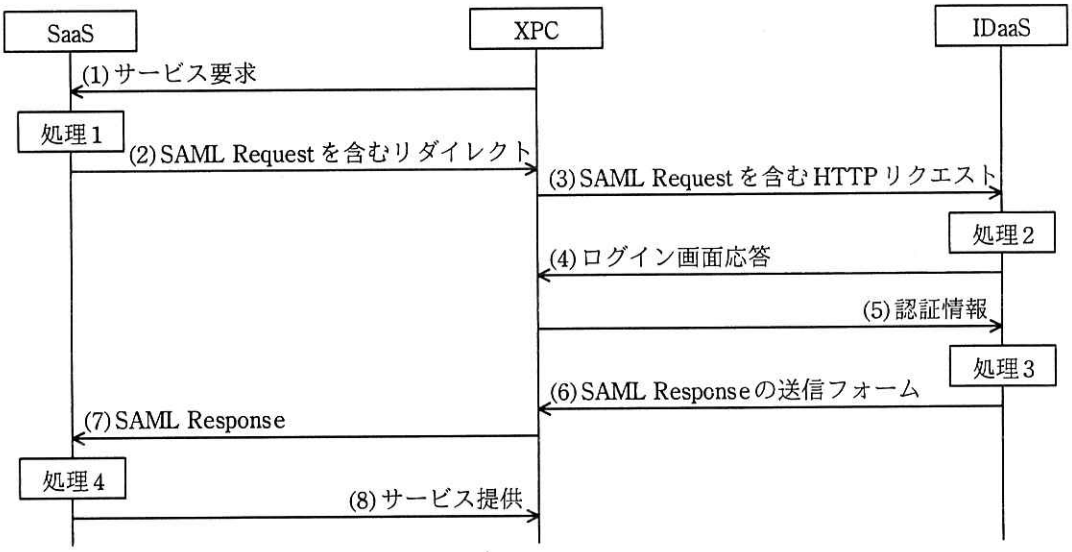


図8　SAML認証の流れ

表2　図8中の各処理の概要

処理名	処理内容
処理1	・IDaaS に認証を要求する SAML Request を生成し，エンコードする。 ・エンコード結果と IDaaS のログイン画面の URL を組み合わせて，リダイレクト先 URL を生成する。
処理2	・図8中の(3)の HTTP リクエスト中の [e] から SAML Request を取得する。 ・信頼関係が構築された SaaS からの認証要求であることを検証する。
処理3	・認証処理を行う。利用者の認証が成功した場合，処理4で用いる SAML アサーションと，それに対するデジタル署名を含めた SAML Response の送信フォームを生成する。
処理4	・SAML Response に含まれるデジタル署名を検証することで，デジタル署名が [f] のものであること，及び SAML アサーションの [g] がないことを確認する。 ・SAML アサーションの内容を検証し，サービス提供すべきかどうかを決定する。

Cさん：事前の準備はありますか。

F氏　：IDaaS と SaaS との間で事前に情報を共有しておく必要があります。事前に共有する情報は，SAML アサーションで用いる属性，図8中の処理 [h] で用いる URL，図8中の処理 [i] 及び処理 [j] において必要なデジタル証明書などがあります。

Cさんは，F氏の提案を受け，SAML 認証をサポートしている IDaaS を調査した。同時に，GrW サービス及びメールサービスを提供し，かつ，SAML 認証をサポートしている SaaS を調査した。調査の結果，G社の SaaS と IDaaS（以下，G社の GrW サービスを GrW-G，メールサービスをメール-G，IDaaS を IDaaS-G という）に移行することを経営陣に提案した。この案は経営陣に承認され，GrW-G 及びメール-G への移行並びに IDaaS-G での SSO の準備が開始された。

〔従業員からの要望〕

GrW-G，メール-G 及び IDaaS-G への移行及び SSO の準備が完了し，利用が開始された 3 か月後に，システム部は，X 社の従業員に対して，GrW-G 及びメール-G についてのヒアリングを実施した。その回答に，GrW-G でスケジュールを管理しているが，会議の主催者が会議日程の調整をもっと簡単にできるようにしてほしいという要望があった。C さんは，S 社が提供しているスケジュール調整サービス（以下，S サービスという）を導入し，GrW-G と連携させることで，その要望に応えることができると考えた。S サービスの内容を表 3 に示す。

表 3　S サービスの内容（抜粋）

項番	項目	内容
1	概要	SaaS で提供されており，S サービスのスマートフォン用アプリケーションプログラム（以下，スマートフォン用アプリケーションプログラムをスマホアプリという）又は PC の Web ブラウザから利用できる。
2	利用手順	(1)　主催者は，S サービスにアクセスする。 (2)　S サービスは，GrW-G から主催者のスケジュールを取得し，空き時間を表示する。 (3)　主催者は，空き時間の中から会議日程の候補を複数選ぶ。 (4)　S サービスは，会議の参加予定者に，各候補に対する参加可否の回答を依頼するメールを送信する。 (5)　会議の参加予定者は，可否を回答する。 (6)　S サービスは，会議の参加予定者の各候補に対する参加可否の一覧表を主催者に示す。 (7)　主催者は，一覧表を見て会議日程を決定する。 (8)　S サービスは，会議の参加予定者に招待メールを送付し，会議日程を GrW-G の主催者のスケジュールに登録する。

C さんは，S サービスの導入検討を進める中で，S サービス，GrW-G 及び IDaaS-G の間の連携について F 氏に相談した。次は，その際の F 氏と C さんの会話である。

F 氏　：S サービス，GrW-G 及び IDaaS-G は，OAuth 2.0 をサポートしています。OAuth 2.0 を利用したサービス要求からスケジュール情報の取得までの流れは，図 9 のようになります。

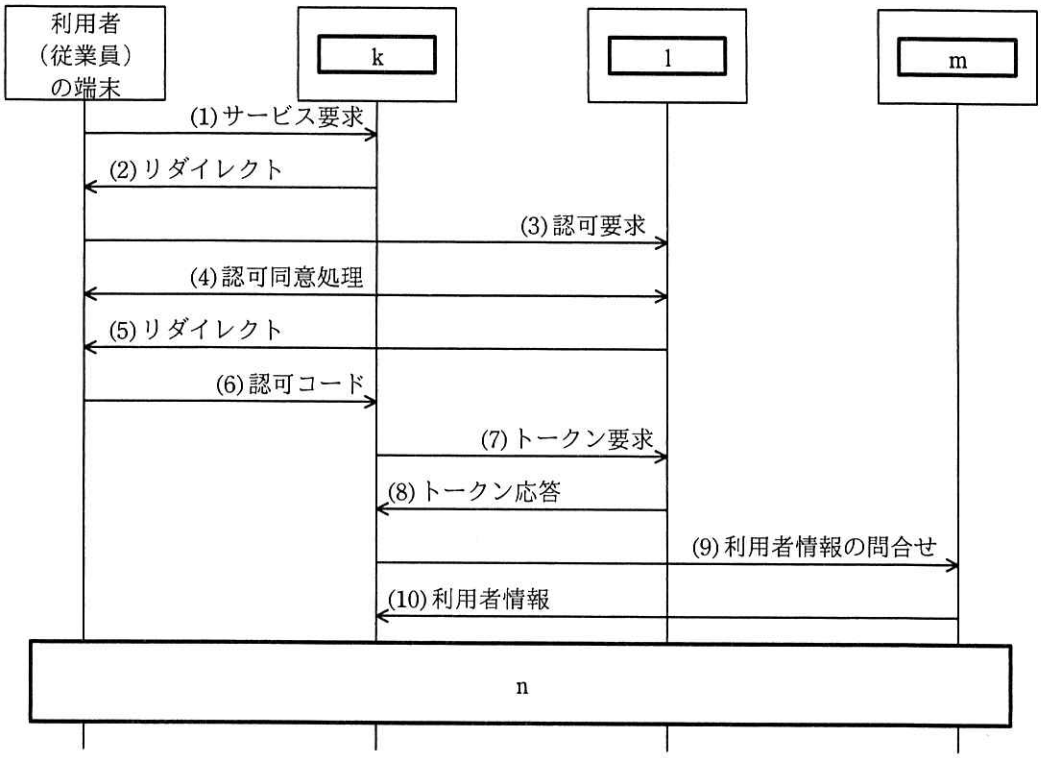


図 9　OAuth 2.0 を利用したサービス要求からスケジュール情報の取得までの流れ

C さん：セキュリティ対策について確認すべきことはありますか。

F 氏　：二つあります。一つ目は，クロスサイトリクエストフォージェリ（以下，CSRF という）攻撃についてです。標的となる利用者が重要な秘密を扱う会議の主催者として日程を決定する場合を考えてみましょう。攻撃者は，GrW-G に攻撃者のアカウントを登録し，当該 GrW-G にアクセスするための認可コードを利用者に送付します。そのときに，図 9 の実装に CSRF脆(ぜい)弱性があり，かつ，利用者の Web ブラウザが攻撃者によって生成された認可コードを受け付けてしまう実装となっている場合，利用者が気付かないうちに攻撃者のアカウントで会議日程が登録されてしまいます。対策として，state パラメタの実装が求められています。適切な実装であれば，図 9 中の [o] において，state パラメタを付与して送信し，図 9 中の [p] で送られてきたものと比較することで，攻撃を検知しているはずです。

二つ目は，利用者が S サービスへのアクセスに S サービスのスマホアプリを

使う場合についてです。S サービスのスマホアプリをインストールしたスマートフォンに，攻撃者が用意した不正なスマホアプリをインストールしてしまうと，GrW-G にアクセスするための認可コードを，攻撃者のスマホアプリが横取りしてしまうという攻撃があります。

C さん：二つ目の攻撃への対策にはどのようなものがありますか。

F 氏　：S サービスのスマホアプリでランダムな検証コードとその値を基にしたチャレンジコードを作成して，そのチャレンジコードを認可要求に追加し，検証コードをトークン要求に追加します。二つのコードを検証することで，検証コードを知らない攻撃者からのトークン要求を排除できます。この仕組みは，[q] として標準化されています。

C さん：分かりました。

〔企画チームからの要望〕

C さんは，企画チームから要望を受けた。要望は，T 社が運営しているメッセージ投稿サイト（以下，T 社投稿サイトという）と X 社動画サーバとを連携させ，T 社投稿サイトの認証サーバを用いた認証機能，及び T 社投稿サイトの投稿サーバへの自動投稿機能を X 社動画サーバに追加したいというものだった。この要望に対応することで，T 社投稿サイトのアカウントをもつ動画サービスの会員は，T 社投稿サイトにログインすれば X 社動画サーバも利用できる。また，X 社動画サーバに動画を投稿すると，“動画の概要”が T 社投稿サイトに自動で投稿されるようにもできる。C さんは，T 社投稿サイトと X 社動画サーバの連携方法について，F 氏に助言を求めた。次は，その際の F 氏と C さんの会話である。

F 氏　：OpenID Connect（以下，OIDC という）を用いれば，T 社投稿サイトと X 社動画サーバを連携できます。例えば，図 10 のような流れです。

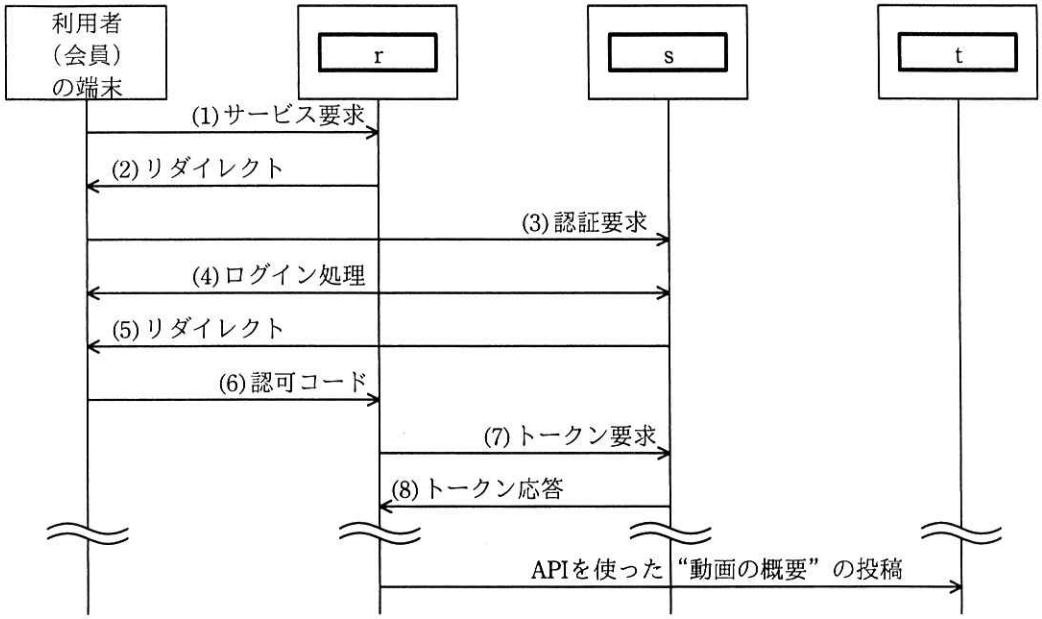


図 10　OIDC を用いた T 社投稿サイトと X 社動画サーバの連携の流れ

F 氏　：認可コードフローの場合，ID トークンは，図 10 中の［　u　］で送付されます。ID トークンは，JSON Web Token 形式で表現され，ヘッダ，ペイロード，署名の三つの部分で構成されます。署名は，ヘッダとペイロードに対して，T 社投稿サイトの認証サーバの秘密鍵を使って作成します。署名アルゴリズムは，ヘッダにおいて指定します。ヘッダ，ペイロード，署名は，それぞれ［　v　］でエンコードされます。

C さん：T 社投稿サイトでのセキュリティ対策について確認することはありますか。

F 氏　：ハイブリッドフローを用いる場合，state パラメタのほか，nonce 値を実装しているかを確認すべきです。まず，nonce 値を生成し，［　w　］に含めて送信します。次に，送られてきた［　x　］に含まれる nonce 値を検証することで，攻撃者による ID トークンの不正利用を防ぐことができます。

C さん：分かりました。

システム部は，T 社投稿サイトと動画サービスとを，OIDC で連携することに決め，X 社動画サーバの改修に着手した。

設問1　〔抜本的な対策の検討〕について，(1)～(5)に答えよ。

(1) 本文中の［ a ］に入れる適切な字句を，5字以内で答えよ。

(2) 本文中の［ b ］に入れる適切な字句を，英字5字以内で答えよ。

(3) 図4中，図5中及び本文中の［ c ］に入れる適切な字句を，英字5字以内で答えよ。

(4) 本文中の下線①について，Y-CDN-U-FQDNを名前解決したIPアドレスを宛先とする通信をFWで拒否した場合に閲覧できなくなるWebサイトの範囲を，60字以内で具体的に述べよ。

(5) 本文中の［ d ］に入れる適切な字句を，20字以内で答えよ。

設問2　〔SSOの現状〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，認証サーバ側では検知することができない理由を，30字以内で述べよ。

(2) 本文中の下線③について，対策にならない理由を，35字以内で述べよ。

設問3　〔SaaSでのSSOの実現〕について，(1)～(4)に答えよ。

(1) 表2中の［ 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　cookie　　イ　HTML　　ウ　クエリ文字列

エ　ボディ　　オ　リファラ

(2) 表2中の［ f ］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　IDaaS　　イ　SaaS　　ウ　XPC

(3) 表2中の［ g ］に入れる適切な字句を，5字以内で答えよ。

(4) 本文中の［ h ］～［ j ］に入れる適切な数字を，それぞれ答えよ。

設問4　〔従業員からの要望〕について，(1)～(4)に答えよ。

(1)　図9中の［ k ］～［ m ］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　GrW-G　　イ　IDaaS-G　　ウ　Sサービス

(2)　図9中の［ n ］に入れる適切な流れを解答群の中から選び，記号で答えよ。

解答群

(3)　本文中の［ o ］，［ p ］に入れる適切な通信を，図9中の(1)～(10)から選び，番号で答えよ。

(4) 本文中の [q] 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 ASLR（Address Space Layout Randomization）

イ EIAM（Enterprise Identity and Access Management）

ウ PKCE（Proof Key for Code Exchange）

エ SCIM（System for Cross-domain Identity Management）

設問5 〔企画チームからの要望〕について，(1)～(4)に答えよ。

(1) 図 10 中の [r] ～ [t] 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 IDaaS-G　　イ S サービス

ウ T 社投稿サイトの投稿サーバ　　エ T 社投稿サイトの認証サーバ

オ X 社動画サーバ

(2) 本文中の [u] に入れる適切な通信を，図 10 中の(1)～(8)から選び，番号で答えよ。

(3) 本文中の [v] 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 base32　　イ base64url

ウ ROT13　　エ UTF-8

(4) 本文中の [w]，[x] に入れる適切な字句を，それぞれ 10 字以内で答えよ。