問２　Web サイトのクラウドサービスへの移行と機能拡張に関する次の記述を読んで，設問に答えよ。

W 社は，従業員 100 名のブログサービス会社であり，日記サービスという Web サービスを 10 年前から提供している。日記サービスの会員は，自分の食事に関する記事の投稿及び摂取カロリーの管理ができる。

日記サービスは，W 社のデータセンター内で稼働している。ハードウェアの調達には 1 か月程度を要する。W 社は，日記サービスが稼働している各機器の運用を D 社に委託している。D 社に委託している運用を表 1 に示す。

表１　D 社に委託している運用（概要）

項番	運用	運用内容
1	ログ保全	・定期的に，日記サービスが稼働している各機器の全てのログを外部メディアにバックアップする。 ・外部メディアにバックアップする前に，ログを一時的に D 社作業用端末にダウンロードする。 ・D 社作業用端末でのバックアップ作業後に，D 社作業用端末からログを削除する。なお，各機器からログを削除する作業は W 社が行う。
2	障害監視	・アプリケーションプログラム（以下，アプリという）の問題の一次切分けを行う。アプリの問題は，ログを監視しているソフトウェアによって検知される。 ・ログを確認して一次切分けを行う。その際に，サーバの一覧を参照する。 ・W 社への連絡は，電子メール（以下，メールという）と電話で行う。
3	性能監視	・W 社が定めた，CPU 稼働率，処理性能及び応答時間に関わる指標（以下，性能指標という）を監視する。 ・異常を検知すると，一次切分けを行う。その際に，サーバの一覧を参照する。 ・必要に応じて，W 社への連絡をメールと電話で行う。
4	機器故障対応	・交換対象のハードウェアの発注を行う。 ・故障機器のハードウェア交換作業を行う。

この 2，3 年，会員が急増しているので，W 社は，日記サービスをクラウドサービスに移行することにした。

〔移行先のクラウドサービス選定〕

W 社は，クラウドサービスへの移行時及び移行後の管理，運用について，検討を開始した。

まず，クラウドサービスへの移行時及び移行後に，W 社が何を管理，運用する必要があるかを調べたところ，表 2 のとおりであった。

表 2　W 社が管理，運用する必要のある範囲

構成要素	クラウドサービスの分類		
	IaaS	PaaS	SaaS
ハードウェア，ネットワーク	×	×	×
OS，ミドルウェア	a	b	c
アプリ	d	e	f
アプリに登録されたデータ	g	h	i

注記　“○”は W 社が管理，運用する必要があるものを示し，“×”は必要がないものを示す。

クラウドサービスへの移行及びクラウドサービスの設定は W 社が行い，移行後，表 1 の項番 1～項番 3 の運用を D 社に委託する計画にした。

移行先のクラウドサービスとして，L 社のクラウドサービスを選定した。L 社が提供しているクラウドサービスを表 3 に示す。

表 3　L 社が提供しているクラウドサービス

クラウドサービス名	説明
仮想マシンサービス	・利用者が OS やアプリを配備することによって，物理サーバと同じ機能を実行するための仮想化基盤である。
データベース（以下，DB という）サービス	・関係 DB である。 ・容量の拡張，バックアップなどは，自動で実行される。
ブロックストレージサービス	・固定長のブロックという論理単位で管理できるストレージである。仮想マシンサービスのファイルシステムとして割り当てることが可能である。
オブジェクトストレージサービス	・データをオブジェクトとして扱い，各オブジェクトをメタデータで管理できるストレージである。 ・オブジェクトの保存のために必要なサーバの資源管理，容量の拡張などは，自動で実行される。
モニタリングサービス	・利用者が利用している L 社の各クラウドサービスについて，性能指標を監視する。

表3　L社が提供しているクラウドサービス（続き）

クラウドサービス名	説明
アラートサービス	・L社のクラウドサービスの環境[1]でイベント[2]が発生したときに，そのイベントを検知してアラートをメールで通知する。
仮想ネットワークサービス	・レイヤー2 スイッチ（以下，L2SW という），ファイアウォール（以下，FW という），ルータなどのネットワーク機器を含むネットワークを仮想的に構成でき，インターネットとの接続を可能にする。

注[1]　L社の各クラウドサービスを利用して構築したシステム及びネットワークを指す。
注[2]　特定の利用者による操作，システム構成の変更，設定変更などである。

イベント検知のルールはJSON形式で記述する。そのパラメータを表4に示す。

表4　イベント検知のルールに記述するパラメータ

パラメータ	内容	取り得る値
system	検知対象とするシステムID	・0000 ～ 9999
account	検知対象とする利用者ID	・0000 ～ 9999
service	検知対象とするクラウドサービス名	・仮想マシンサービス ・オブジェクトストレージサービス ・モニタリングサービス
event	検知対象とするイベント	eventの取り得る値は，serviceの値によって異なる。 ・仮想マシンサービスの場合 － 仮想マシンの起動 － 仮想マシンの停止 － 仮想マシンの削除 ・オブジェクトストレージサービスの場合 － オブジェクトの作成 － オブジェクトの編集 － オブジェクトの削除 － オブジェクトの閲覧 － オブジェクトのダウンロード ・モニタリングサービスの場合 － 監視する性能指標の追加 － 監視する性能指標の削除

注記　systemとaccountの取り得る値には正規表現を利用できる。正規表現は次の規則に従う。
[012] は，0，1又は2のいずれか数字1文字を表す。
[0-9] は，0から9までの連続する数字のうち，いずれか数字1文字を表す。
* は，直前の正規表現の0回以上の繰返しを表す。
+ は，直前の正規表現の1回以上の繰返しを表す。

仮想マシンサービスを利用して構築した，システムIDが0001のシステムにおいて，

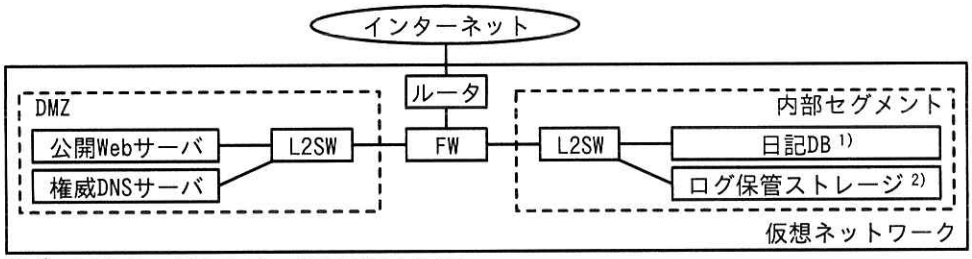
利用者 ID が 1000 である利用者が仮想マシンを停止させた場合の，イベント検知のルールの例を図 1 に示す。

```
1: {
2:  "system": "0001",
3:  "account": "1000",
4:  "service": "仮想マシンサービス",
5:  "event": "仮想マシンの停止"
6: }
```

図 1　イベント検知のルールの例

〔日記サービスの L 社のクラウドサービスへの移行〕

移行後の日記サービスの仮想ネットワーク構成を図 2 に，図 2 中の主な構成要素を表 5 に示す。



注 1)　日記サービスのデータを管理する DB
注 2)　日記サービスのログを保管するストレージ

図 2　移行後の日記サービスの仮想ネットワーク構成

表 5　図 2 中の主な構成要素

システム ID	構成要素	利用する L 社のクラウドサービス
1000	公開 Web サーバ	・仮想マシンサービス ・ブロックストレージサービス
2000	権威 DNS サーバ	・仮想マシンサービス ・ブロックストレージサービス
3000	日記 DB	・DB サービス
4000	ログ保管ストレージ	・オブジェクトストレージサービス
5000	仮想ネットワーク	・仮想ネットワークサービス

注記　日記サービスでは，モニタリングサービスとアラートサービスを利用する。

W 社は，L 社のクラウドサービスにおける，D 社に付与する権限の検討を開始した。

〔L 社のクラウドサービスにおける権限設計〕

L 社の各クラウドサービスにおける権限ごとに可能な操作を表 6 に示す。

表 6　L 社の各クラウドサービスにおける権限ごとに可能な操作（抜粋）

クラウドサービス名	一覧の閲覧権限	閲覧権限	編集権限
仮想マシンサービス	仮想マシン一覧の閲覧	仮想マシンに割り当てたファイルシステム上のファイルの閲覧	・仮想マシンの起動，停止，削除 ・仮想マシンへのファイルシステムの割当て ・仮想マシンに割り当てたファイルシステム上のファイルの作成，編集，削除 ・仮想マシンの性能の指定
DB サービス	スキーマ一覧及びテーブル一覧の閲覧	テーブルに含まれるデータの閲覧	・テーブルの作成，編集，削除 ・テーブルに含まれるデータの追加，編集，削除
ブロックストレージサービス	生成したストレージ一覧の閲覧	ストレージの使用済み容量及び空き容量の閲覧	・ストレージの生成 ・ストレージの容量の指定
オブジェクトストレージサービス	オブジェクト一覧の閲覧	オブジェクトの閲覧	・オブジェクトの作成，編集，削除 ・オブジェクトのダウンロード
モニタリングサービス	監視している性能指標一覧の閲覧	過去から現在までの性能指標の値の閲覧	・監視する性能指標の追加，削除

W 社は，D 社に付与する権限が必要最小限となるように，表 7 に示す D 社向けの権限のセットを作成した。

表 7　D 社向けの権限のセット（抜粋）

クラウドサービス名	D 社に付与する権限
仮想マシンサービス	j
DB サービス	k
オブジェクトストレージサービス	一覧の閲覧権限，閲覧権限，編集権限
モニタリングサービス	l

さらに，W 社は，①D 社の運用者がシステムから日記サービスのログを削除したときに，そのイベントを検知してアラートをメールで通知するための検知ルールを作成した。

W 社は，L 社とクラウドサービスの利用契約を締結して，日記サービスを L 社のクラウドサービスに移行し，運用を開始した。

〔機能拡張の計画開始〕

W 社は，サービス拡大のために，機能を拡張した日記サービス（以下，新日記サービスという）の計画を開始した。新日記サービスの要件は次のとおりである。

要件 1：会員が記事を投稿する際，他社の SNS にも同時に投稿できること

要件 2：スマートフォン用のアプリ（以下，スマホアプリという）を提供すること

W 社は，要件 1 を実装した後で要件 2 に取り組むことに決めた。その上で，要件 1 を実現するために，T 社の SNS（以下，サービス T という）と連携することにした。

〔サービス T との連携の検討〕

OAuth 2.0 を利用してサービス T と連携した場合のサービス要求から記事投稿結果取得までの流れを図 3 に，送信されるデータを表 8 に示す。

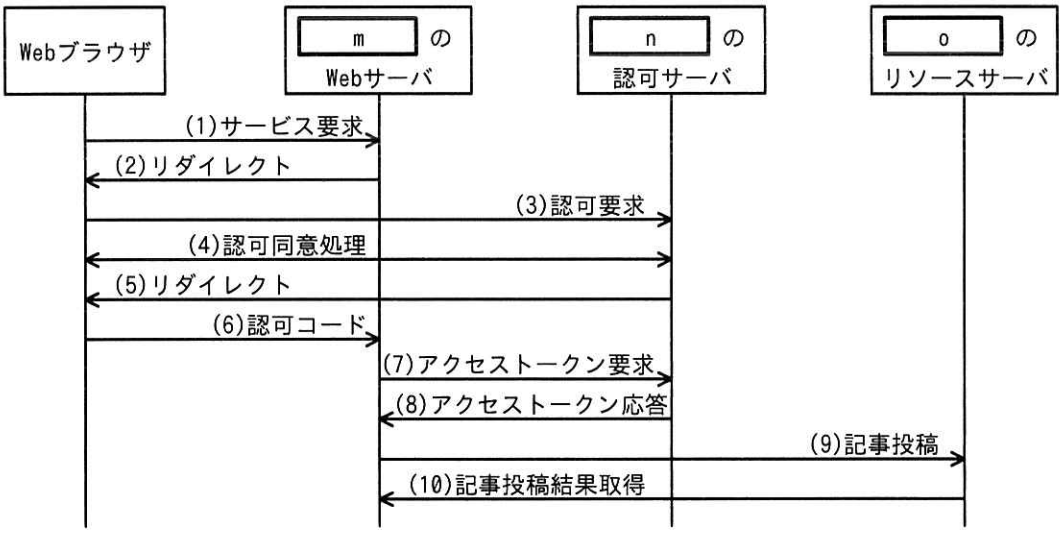


図 3　サービス要求から記事投稿結果取得までの流れ

表8　送信されるデータ（抜粋）

番号	送信されるデータ
p	GET /authorize?response_type=code&client_id=abcd1234&redirect_uri=https://△△△.com/callback HTTP/1.1 [1]
q	POST /oauth/token HTTP/1.1 Authorization: Basic YWJjZDEyMzQ6UEBzc3dvcmQ= [2] grant_type=authorization_code&code=5810f68ad195469d85f59a6d06e51e90&redirect_uri=https://△△△.com/callback

注記　△△△.com は，新日記サービスのドメイン名である。

注[1]　クエリ文字列中の“abcd1234”は，英数字で構成された文字列であるクライアント ID を示す。

注[2]　“YWJjZDEyMzQ6UEBzc3dvcmQ=”は，クライアント ID と，英数字と記号で構成された文字列であるクライアントシークレットとを，“:”で連結して base64 でエンコードした値（以下，エンコード値 G という）である。

各リクエストの通信で TLS 1.2 及び TLS 1.3 を利用可能とするために，②暗号スイートの設定をどのようにすればよいかを検討した。また，サービス T との連携のためのモジュール（以下，R モジュールという）の実装から単体テストまでを F 社に委託することにした。F 社は，新技術を積極的に活用している IT 企業である。

〔F 社の開発環境〕

F 社では，R モジュールの開発は，取りまとめる開発リーダー1 名と，実装から単体テストまでを行う開発者 3 名のチームで行う。システム開発において，顧客から開発を委託されたプログラムのソースコードのリポジトリと外部に公開されている OSS リポジトリを利用している。二つのリポジトリは，サービス E というソースコードリポジトリサービスを利用して管理している。

サービス E の仕様と，R モジュールについての F 社のソースコード管理プロセスは，表 9 のとおりである。

表9　サービスEの仕様とF社のソースコード管理プロセス

機能	サービスEの仕様	F社のソースコード管理プロセス
利用者認証及びアクセス制御	・利用者 ID とパスワードによる認証，及び他の IdP と連携した SAML 認証が可能である。 ・リポジトリごとに，利用者認証の要・不要を設定できる。 ・サービスEは外部に公開されている。 ・IP アドレスなどで接続元を制限する機能はない。	・利用者認証には，F 社内で運用している認証サーバと連携した，SAML 認証を利用する。 ・R モジュール開発向けのリポジトリ（以下，リポジトリ W という）には，利用者認証を“要”に設定する。
バージョン管理	・ソースコードのアップロード[1]，承認，ダウンロード，変更履歴のダウンロード，削除が可能である。 ・新規作成，変更，削除の前後の差分をソースコードの変更履歴として記録する。 ・ソースコードがアップロードされ，承認されると，対象のソースコードが新バージョンとして記録され，変更履歴のダウンロードが可能になる。	・開発者は，静的解析と単体テストを実施する。開発者が，それら二つの結果とソースコードをアップロードして，開発リーダーに承認を依頼するルールとする。ただし，静的解析と単体テストについてリスクが少ないと開発者が判断した場合は，開発者自身がソースコードのアップロードとその承認の両方を実施できるルールとする。
権限管理	・設定できる権限には，ソースコードのダウンロード権限，ソースコードのアップロード権限，アップロードされたソースコードを承認する承認権限がある。 ・利用者ごとに，個別のリポジトリの権限を設定することが可能である。 ・変更履歴のダウンロードには，ソースコードのダウンロード権限が必要である。 ・変更履歴の削除には，アップロードされたソースコードを承認する承認権限が必要である。 ・外部のX社が提供している継続的インテグレーションサービス[2]（以下，X社CIという）と連携するには，ソースコードのダウンロード権限をX社CIに付与する必要がある。	・開発者，開発リーダーなど全ての利用者に対して，設定できる権限全てを与える。
サービス連携	・別のクラウドサービスと連携する際に，権限を付与するトークン（以下，E トークンという）を，リポジトリへアクセスしてきた連携先に発行することができる。 ・E トークンの有効期間は1か月である。E トークンの発行形式や有効期間の変更はできない。	・X社CIと連携する。 ・X社CIに発行するEトークン（以下，X トークンという）には，リポジトリWの全ての権限が付与されている。

注記　OSS リポジトリには，利用者認証を“不要”に設定している。また，OSS リポジトリのソースコードと変更履歴のダウンロードは誰でも可能である。

注[1]　ソースコードのアップロードには，関連するファイルの新規作成，変更，削除の操作が含まれる。

注[2]　アップロードされたソースコードが承認されると，ビルドと単体テストを自動実行するサービスである。

〔悪意のある不正なプログラムコードの混入〕

F 社は，R モジュールの実装について単体テストまでを完了して，ソースコードを W 社に納品した。その後，W 社と T 社は結合テストを開始した。

結合テスト時，外部のホストに対する通信が R モジュールから発生していることが分かった。調べたところ，不正なプログラムコード（以下，不正コード M という）がソースコードに含まれていたことが分かった。不正コード M は，OS の環境変数の一覧を取得し，外部のホストに送信する。新日記サービスでは，エンコード値 G が OS の環境変数に設定されていたので，その値が外部のホストに送信されていた。

W 社は，漏えいした情報が悪用されるリスクの分析と評価を行うことにした。それと並行して，不正コード M の混入の原因調査と，プログラムの修正を F 社に依頼した。

〔W 社によるリスク評価〕

W 社は，リスクを分析し，評価した。評価結果は次のとおりであった。

・エンコード値 G を攻撃者が入手した場合，[m] の Web サーバであると偽ってリクエストを送信できる。しかし，図 3 のシーケンスでは，③攻撃者が特定の会員のアクセストークンを取得するリクエストを送信し，アクセストークンの取得に成功することは困難である。

次に，W 社は，近い将来に要件 2 を実装する場合におけるリスクについても，リスクへの対応を検討した。

そのリスクのうちの一つは，スマホアプリのリダイレクトにカスタム URL スキームを利用する場合に発生する可能性がある。W 社が提供するスマホアプリと攻撃者が用意した偽のスマホアプリの両方を会員が自分の端末にインストールしてしまうと，正規のスマホアプリとサーバとのやり取りが偽のスマホアプリに横取りされ，攻撃者がアクセストークンを不正に取得できるというものである。この対策として，PKCE（Proof Key for Code Exchange）を利用すると，偽のスマホアプリにやり取りが横取りされても，アクセストークンの取得を防ぐことができる。

要件 2 を実装する場合のサービス要求から記事投稿結果取得までの流れを図 4 に示す。

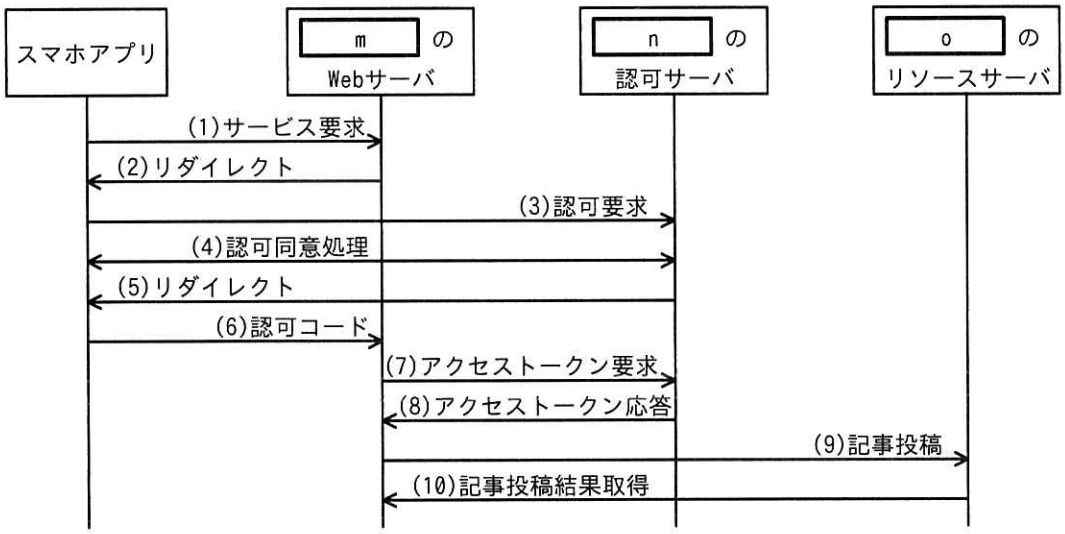


図4　要件2を実装する場合のサービス要求から記事投稿結果取得までの流れ

PKCE の実装では，乱数を基に，チャレンジコードと検証コードを生成する。(3)のリクエストにチャレンジコードと code_challenge_method パラメータを追加し，(7)のリクエストに検証コードパラメータを追加する。最後に，④認可サーバが二つのコードの関係を検証することで，攻撃者からのアクセストークン要求を排除できる。

〔F 社による原因調査〕

F 社は，不正コード M が混入した原因を調査した。調査の結果，サービス E の OSS リポジトリ上に，X トークンなどの情報が含まれるファイル（以下，ファイル Z という）がアップロードされた後に削除されていたことが分かった。

F 社の開発者の 1 人が，ファイル Z を誤ってアップロードし，承認した後，誤ってアップロードしたことに気付き，ファイル Z を削除した上で開発リーダーに連絡していた。開発リーダーは，ファイル Z が OSS リポジトリから削除されていること，ファイル Z がアップロードされてから削除されるまでの間にダウンロードされていなかったことを確認して，問題なしと判断していた。

F 社では，⑤第三者が X トークンを不正に取得して，リポジトリ W に不正アクセスし，不正コード M をソースコードに追加したと推測した。そこで，F 社では，X トークンを無効化し，次の再発防止策を実施した。

・表 9 中のバージョン管理に関わる見直しと⑥表 9 中の権限管理についての変更

・X トークンが漏えいしても不正にプログラムが登録されないようにするための，⑦表 9 中のサービス連携に関わる見直し

ソースコードには他の不正な変更は見つからなかったので，不正コード M が含まれる箇所だけを不正コード M が追加される前のバージョンに復元した。

W 社は，F 社が改めて納品した R モジュールに問題がないことを確認し，新日記サービスの提供を開始した。

設問 1　表 2 中の [a] ～ [i] に入れる適切な内容を，“○”又は“×”から選び答えよ。

設問 2　〔L 社のクラウドサービスにおける権限設計〕について答えよ。

(1)　表 7 中の [j] ～ [l] 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　一覧の閲覧権限，閲覧権限，編集権限

イ　一覧の閲覧権限，閲覧権限

ウ　一覧の閲覧権限

エ　なし

(2)　本文中の下線①のイベント検知のルールを，JSON 形式で答えよ。ここで，D 社の利用者 ID は，1110～1199 とする。

設問 3　〔サービス T との連携の検討〕について答えよ。

(1)　本文中，図 3 中及び図 4 中の [m] ～ [o] に入れる適切な字句を，“新日記サービス”又は“サービス T”から選び答えよ。

(2)　表 8 中の [p]，[q] に入れる適切な番号を，図 3 中の番号から選び答えよ。

(3) 本文中の下線②について，CRYPTREC の“電子政府推奨暗号リスト（令和 4 年 3 月 30 日版)”では利用を推奨していない暗号技術が含まれる TLS 1.2 の暗号スイートを，解答群の中から全て選び，記号で答えよ。

解答群

ア TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

イ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

ウ TLS_RSA_WITH_3DES_EDE_CBC_SHA

エ TLS_RSA_WITH_RC4_128_MD5

設問４ 〔W 社によるリスク評価〕について答えよ。

(1) 本文中の下線③について，アクセストークンの取得に成功することが困難である理由を，表 8 中のパラメータ名を含めて，40 字以内で具体的に答えよ。

(2) 本文中の下線④について，認可サーバがチャレンジコードと検証コードの関係を検証する方法を，“ハッシュ値を base64url エンコードした値”という字句を含めて，70 字以内で具体的に答えよ。ここで，code_challenge_method の値は S256 とする。

設問５ 〔F 社による原因調査〕について答えよ。

(1) 本文中の下線⑤について，第三者が X トークンを取得するための操作を，40 字以内で答えよ。

(2) 本文中の下線⑥について，権限管理の変更内容を，50 字以内で答えよ。

(3) 本文中の下線⑦について，見直し後の設定を，40 字以内で答えよ。