問2　クラウド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 1，2 に答えよ。

U 社は，東京に本社をもつ従業員数 1,000 名の商社である。複数の海外拠点を設置し，海外向けに営業展開している。海外拠点の従業員数は 1 拠点当たり十数名ほどである。

本社の情報システムは，本社の情報システム部が管理しており，各海外拠点の情報システムは，現地の情報システム担当者が管理している。電子メール（以下，メールという）の送受信には，本社ではオンプレミス環境を導入しているが，海外拠点では，P 社が提供するクラウドサービス型 Web メールサービス（以下，メールサービス P という）を利用している。海外拠点では，全ての従業員にスマートフォンとノート PC を貸与している。

〔セキュリティインシデント発生〕

1 月 10 日，送信者が海外拠点 Q の従業員 S さんのメールアドレスである不審なメールを受け取ったという連絡が，S さんとやり取りのあった本社の従業員から情報システム部にあった。情報システム部では，情報処理安全確保支援士（登録セキスペ）である T さんが，調査を担当することになった。T さんが当該メールのヘッダ情報を確認したところ，メールサービス P から送信されたものであった。

海外拠点 Q の情報システム担当者である Y さんによれば，1 月 10 日に S さんのアカウントからの不審なメール送信と考えられる履歴が複数残っているとのことであった。そこで，T さんは，Y さんにメールサービス P の S さんのアカウントを一時的に無効化するよう依頼した。また，会社から貸与された S さんのスマートフォン及びノート PC 並びに S さんのメールボックスには重要情報がなかったことを確認した。T さんが，海外拠点 Q の全従業員のアカウントについて，メールサービス P に残っていた全てのメール送信履歴を Y さんに確認してもらったところ，S さんのアカウント以外に不審なメールの送信履歴はないとのことであった。

〔経緯の調査〕

T さんは，メールサービス P に残っていた海外拠点 Q の全従業員のアカウントのメール送信履歴及び監査ログ，並びに S さんへのヒアリングの結果を Y さんから送付

してもらい，調査した。調査結果を図1に示す。

・1月10日は，Sさんはアジアの Z 国に出張中だった。
・U 社には，会社から貸与されたノート PC を U 社以外の無線 LAN に接続してはならないというルールがあるが，S さんはそのルールを知らず，その日，出張先のホテルで宿泊客用の無線 LAN（以下，ホテル Wi-Fi という）を利用していた。
・ホテル Wi-Fi の SSID は，宿泊客で共通であり，その SSID と事前共有鍵はロビーなどの共有スペースに張り出されていた。
・S さんのノート PC（以下，PC-S という）は，IP アドレス及び DNS サーバの情報を DHCP で自動取得する設定になっていた。
・S さんは，その日，メールサービス P を利用するために，Web ブラウザのアドレスバーにメールサービス P の FQDN を手入力し，ログインページに利用者 ID とパスワードを入力した。
・S さんがメールサービス P にアクセスした時，サーバ証明書が信頼できない旨のエラーは Web ブラウザ上に表示されなかった。
・メールサービス P の監査ログに記録されていた S さんの利用者 ID によるログイン記録のうち不審メールが送信されていた時間帯のものは，Z 国，及び S さんが出張していない南米の W 国の IP アドレスからのものだった。

図1　調査結果（抜粋）

T さんが調べたところ，メールサービス P は HTTP over TLS でサービスが提供されている。HTTP でアクセスした場合は HTTP over TLS の URL にリダイレクトされる仕様になっており，HSTS（HTTP Strict Transport Security）は実装されていない。

こうしたことから，T さんは S さんが不正アクセスを受けたと確信し，図2に示す手口（以下，手口 G という）を使って，攻撃者がメールサービス P の S さんの利用者 ID で不正アクセスしたと推測した。

・攻撃者は，①無線 LAN アクセスポイント，DNS サーバ及び Web サーバを用意した。その DNS サーバには［ a ］の FQDN と［ b ］の IP アドレスとを関連付ける A レコードが設定されていた。
・S さんは，PC-S をホテル Wi-Fi に接続しようとして，攻撃者が用意した無線 LAN アクセスポイントに接続してしまった。
・その結果，PC-S に攻撃者が用意した DNS サーバの情報が設定された。
・S さんは，Web ブラウザからメールサービス P にアクセスしたつもりだったが，実際には Web ブラウザは②攻撃者が用意した Web サーバに接続していた。S さんは，サーバ証明書が信頼できない旨のエラーが表示されなかったので，その Web サーバに対して，利用者 ID 及びパスワードを入力してしまった。
・攻撃者は盗んだ S さんの利用者 ID 及びパスワードを使ってメールサービス P に不正アクセスした。

図2　手口 G

Tさんは，今回のセキュリティインシデントの調査結果を情報システム部長に報告した。情報システム部長は，会社から貸与されたノートPCをU社以外の無線LANに接続してはならないというルールの全社への周知及びメールサービスPの認証方式の強化をTさんに指示した。

〔認証方式の強化〕

情報システム部長からメールサービスPの認証方式の強化について，次の2点が要求された。

要求1　U社以外の無線LANに接続したとしても手口Gを防ぐこと

要求2　手口Gに限らず，偽サイトにアクセスしてしまったときにフィッシングの手口によるメールサービスPへの不正アクセスを防ぐこと

Tさんが調査したところ，メールサービスPは，単体ではパスワード認証にしか対応していないが，認証連携の機能があることが分かった。認証連携機能を使えば，メールサービスPにアクセスしようとしたときに，他のID管理サービスにリダイレクトされ，そこで認証が行われ，認証に成功すると，メールサービスPにアクセスできるようになる。そこで，X社が提供するクラウドサービス型ID管理サービス（以下，IDaaS-Xという）が対応している，より強力な認証方式を利用することにした。IDaaS-Xでは，認証サーバXを使って利用者を認証する。

IDaaS-Xが対応している，より強力な認証方式には，次の2種類がある。

・ワンタイムパスワード（以下，OTPという）認証方式

TOTP（Time-based One-Time Password algorithm）用のスマートフォンアプリケーションプログラム（以下，TOTPアプリという）を利用した認証方式

・パスワードレス認証方式

WebAuthn（Web Authentication API）対応のWebブラウザ及び生体認証対応のオーセンティケータを搭載したデバイスを利用した認証方式

Tさんは二つの認証方式について，要求1及び要求2を満たすことができるかを検討した。

T さんは，まず OTP 認証方式を検討した。IDaaS-X における TOTP アプリ登録処理を図 3 に，OTP 認証方式の認証処理を図 4 に示す。

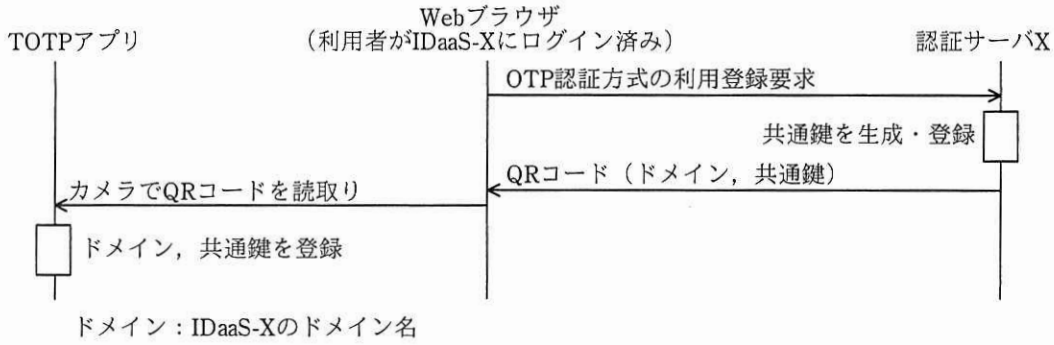


図 3　IDaaS-X における TOTP アプリ登録処理

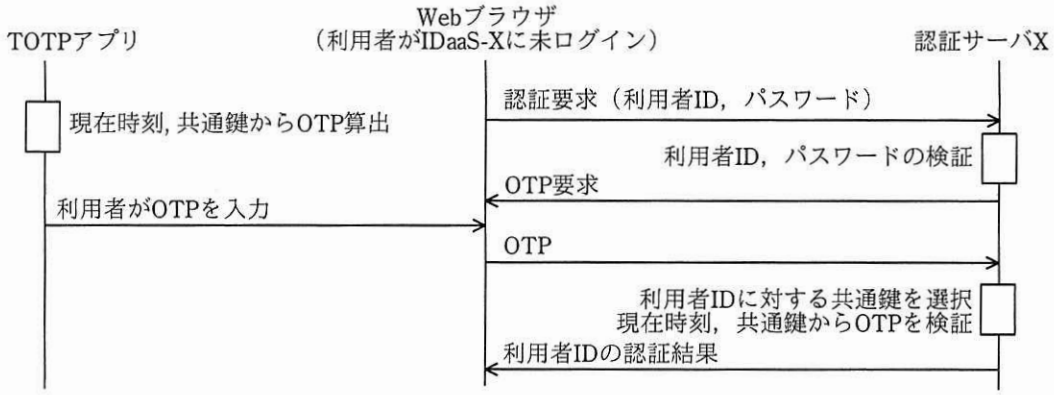
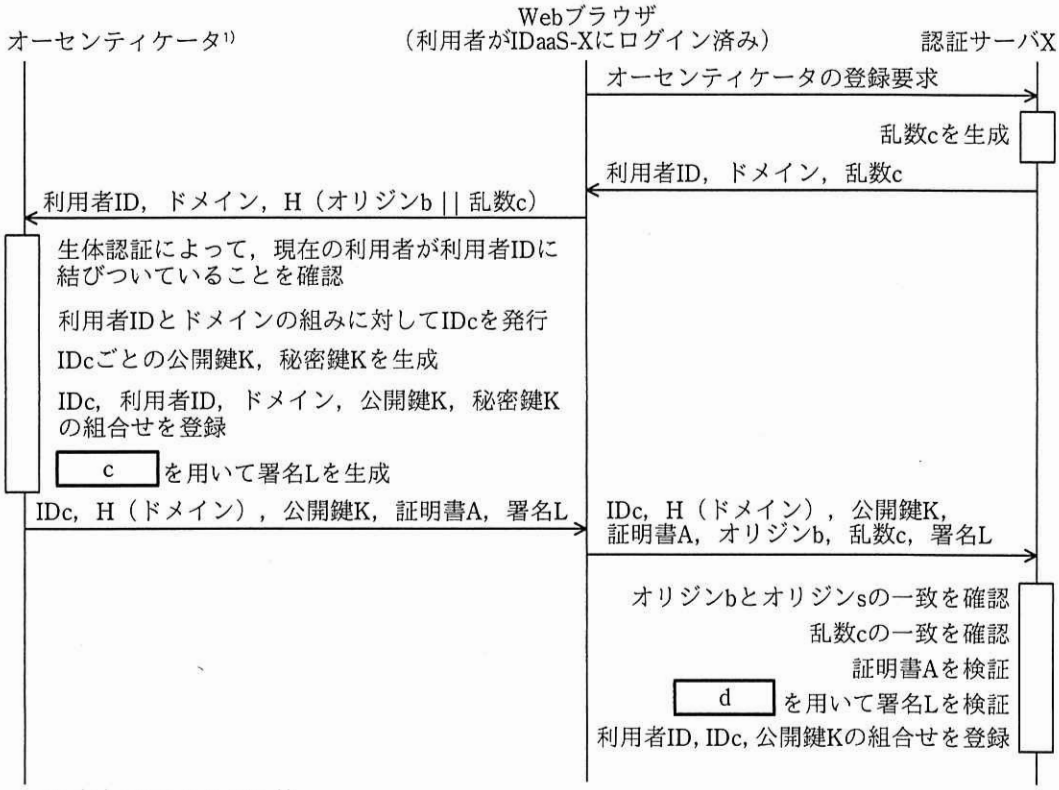


図 4　IDaaS-X における OTP 認証方式の認証処理

OTP 認証方式を利用した場合，ログインには時刻によって変化する OTP も必要になるので，パスワードが窃取された場合でも不正ログインを防ぐことが可能となる。しかし，③OTP 認証方式を利用し，かつ，登録処理を正しく行ったとしても，要求 2 を満たすことができないおそれがある。

次に T さんは，パスワードレス認証方式を検討した。IDaaS-X におけるオーセンティケータ登録処理を図 5 に，認証処理を図 6 に示す。



H（A）：Aのハッシュ値

A || B：AとBを連結

オリジンb：Webブラウザがアクセスしたwebサイトのオリジン

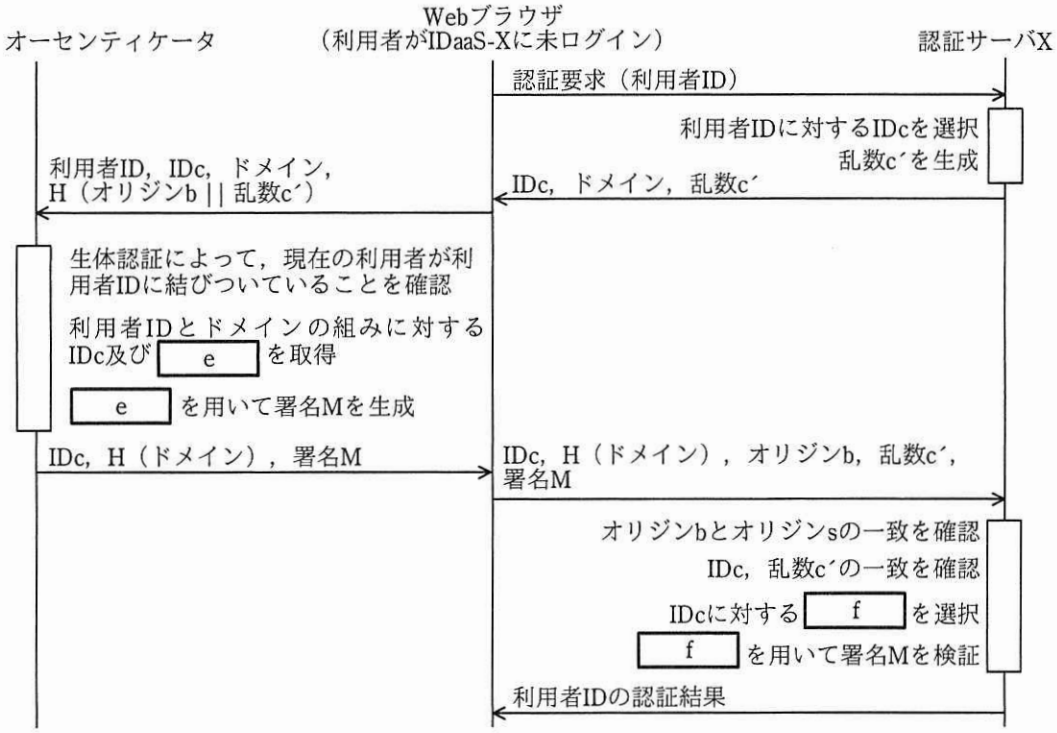
オリジンs：認証サーバXのWebサイトのオリジン

IDc：利用者IDとドメインの組みに対して，オーセンティケータごとに発行されるID

署名L：IDc，H（ドメイン），公開鍵K，H（オリジンb || 乱数c）に対するディジタル署名

注 1) オーセンティケータには，搭載されたデバイスごとにユニークな公開鍵 A，秘密鍵 A，及び証明書 A が組み込まれている。ここで，証明書 A は，信頼された認証局が発行した，公開鍵 A に対するディジタル証明書である。

図 5　IDaaS-X におけるオーセンティケータ登録処理



署名M：H（ドメイン），H（オリジンb || 乱数c´）に対するディジタル署名

図6　IDaaS-Xにおけるパスワードレス認証方式の認証処理

④パスワードレス認証方式を利用すれば，要求2を満たすことができると考えられた。

Tさんは，検討結果を情報システム部長に報告した。情報システム部長は，海外拠点Qにおけるメールサービスpへのパスワードレス認証方式の導入を，Tさん及びYさんに指示した。

海外拠点で従業員に貸与しているスマートフォンとノートPCにはオーセンティケータが搭載されていたので，パスワードレス認証方式を速やかに導入することができた。

U社では，他の海外拠点でのクラウドサービスについても，同様の方式を導入することにした。

設問1　〔経緯の調査〕について，(1)～(3)に答えよ。

(1)　図2中の下線①について，攻撃者が用意した無線LANアクセスポイントには何が設定されていたと考えられるか。設定を30字以内で述べよ。

(2)　図2中の［　a　］，［　b　］に入れる適切な字句を，本文，図1又は図2中の字句を用いて答えよ。

(3)　図2中の下線②について，この時，サーバ証明書が信頼できない旨のエラーが表示されなかったのはなぜか。メールサービスPにHSTSが実装されていないことを踏まえ，理由を20字以内で述べよ。

設問2　〔認証方式の強化〕について，(1)～(3)に答えよ。

(1)　本文中の下線③について，偽サイトにおいてどのような処理が行われればメールサービスPへの不正アクセスが成立するか。行われる処理を35字以内で述べよ。

(2)　図5及び図6中の［　c　］～［　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　公開鍵A　　イ　公開鍵K　　ウ　秘密鍵A　　エ　秘密鍵K

(3)　本文中の下線④について，理由を図5又は図6中の字句を用いて，40字以内で述べよ。