め込んで利用者に送る処理が必用である。それに加えて、サイト X では行われていないことから脆弱性となっていた、トークンを利用者 ID 等とひも付けする処理、そして、利用者から返されたトークンを検証する処理が考えられる。

＜問２＞　クラウドサービスへの移行

●設問１

［試験センターによる解答例］

(1) a：キャッシュ（5 字）

(2) b：DDoS（4 字）

(3) c：Host（4 字）

(4) Y-CDN-U-FQDN を名前解決した IP アドレスと同じ IP アドレスをもつ Web サイト（43 字）

(5) d：TLS の接続先サーバ名（11 字）

＜解説＞

(1) CDN とは、Web サイトの静的コンテンツを、CDN サービスプロバイダが管理・運営する複数のキャッシュサーバに分散配置することにより、表示速度の高速化や負荷分散を図る技術である。

(2) CDN により、Web コンテンツが分散されるため、特定の Web サイトに集中攻撃を仕掛ける DDoS 攻撃への耐性が向上する。

(3) HTTP リクエストにおいて、接続先のサーバの URI、ポート番号等の情報を指定するのは Host ヘッダである。

(4) 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 で拒否した場合は、Y-CDN-U-FQDN を名前解決した IP アドレスと同じ IP アドレスをもつ Web サイトが閲覧できなくなる。

(5) 図5にあるように､ドメインフロンティング攻撃では､TLSの接続先サーバ名と、HTTP リクエストの Host ヘッダに異なる接続先情報を設定することで、不正な通信を行っている。したがって､それら 2 つの情報が一致していることを検証し、一致していなければ遮断することで対策が可能である。

●設問２

［試験センターによる解答例］

(1) ST は認証サーバに送られないから（16 字）

(2) 総当たり攻撃はオフラインで行われ、ログインに失敗しないから（29 字）

＜解説＞

(1) Kerberos では、ST は認証サーバから発行されると、以降はクライアントとサービス提供するサーバとの間でやり取りされ、認証サーバに送られることはない。したがって、もし ST が偽造されたとしても、認証サーバで検知することはできない。

(2) 図 7 の注記にあるように、ST はサーバ管理者アカウントのパスワードのハッシュ値を鍵として暗号化されており、攻撃者は同パスワードを手に入れるため総当たり攻撃を行う。この攻撃は ST に対して直接オフラインで行われるため、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らない。

●設問３

［試験センターによる解答例］

(1) e：ウ

(2) f：ア

(3) g：偽造（2 字）

(4) h：1
i：3
j：4
※i と j は順不同。

＜解説＞

(1) SAML Request は HTTP リクエストのクエリ文字列に含まれており、IDaaS はそれを取得して処理を行う。

(2) SAML Response に含まれるデジタル署名は IDaaS によって付与されたものなので、それを検証する。

(3) デジタル署名を検証するもう一つの目的は、SAML Response に偽造がないかどうかの確認である。

(4) h：表 2 の処理 1 にてリダイレクト先 URL を生成していることからわかるように、URL を用いるのは処理 1 である。

i、j：表 2 の処理 3 でデジタル署名を生成し、処理 4 でその検証を行っていることからわかるように、デジタル証明書を用いるのは処理 3 と処理 4 である。

●設問４

［試験センターによる解答例］

(1) k：**ウ**
l：**イ**
m：**ア**

(2) n：**エ**

(3) o：(2)
p：(6)

(4) q：**ウ**

＜解説＞

(1) 図 9 で、利用者の端末が最初にサービス要求を送る先なので、[k]は S サービスである。その後、(3)で認可要求、(7)でトークン要求を送る先となっている[l]は、IDaaS-G である。そして(10)で利用者情報を S サービスに送っている[m]が GrW-G である。

(2) 利用者情報に続いてスケジュール情報を取得する処理であるため、(9)、(10)と同様に、S サービスと GrW-G との間で行われることになる。したがってエが正しい。

(3) 問題文のような攻撃を検知するには、図 9(1)のサービス要求に対する(2)のリダイレクトにおいて state パラメタを付与して利用者端末に送信し、その後(6)で認可コードと state パラメタを利用者端末が送るようにすればよい。

(4) 問題文にあるような認可コードの横取り対策として標準化されているのは、PKCE（ピクシー）である。PKCE は OAuth2.0 の拡張仕様であり、RFC 7636 に "Proof Key for Code Exchange by OAuth Public Clients"として定義されている。

●設問５

［試験センターによる解答例］

(1) r：**オ**
　　s：**エ**
　　t：**ウ**

(2) u：(8)

(3) v：**イ**

(4) w：**認証要求（4 字）**
　　x：**ID トークン（6 字）**

＜解説＞

(1) 図 10 は OIDC による T 社投稿サイトと X 社動画サーバ連携の流れであり、末尾の処理で［ r ］から［ t ］に対して"動画の概要"の投稿が行われていることから、［ r ］には X 社動画サーバ、［ t ］には T 社投稿サイトの投稿サーバが入ることがわかる。また、利用者の端末からの認証要求や X 社動画サーバからのトークン要求を処理している［ s ］は、T 社投稿サイトの認証サーバである。

(2) ID トークンの送付であるから、該当するのは(8)のトークン応答である。

(3) エンコードで標準的に用いられているのは base64 である。base64url は、URL を base64 エンコードした場合に特定の文字（"+", "/"）で問題が生じるのを防ぐための仕様を追加した方式である。

(4) 攻撃者により ID トークンが不正利用されるのを防ぐために使用されるのが nonce 値である。まず、利用者の端末で生成した nonce 値を認証要求に含めて送信する。その後、送られてきたトークン ID に含まれる nonce 値を検証することで、不正利用を防ぐ。