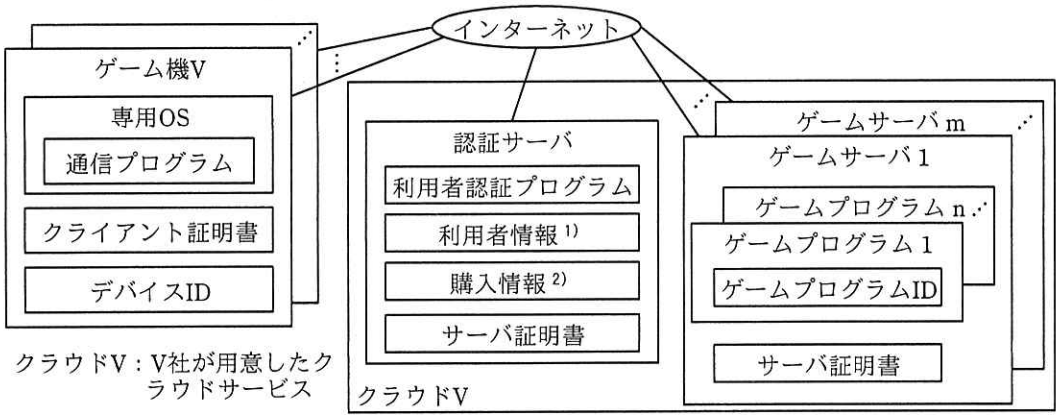
問３　IoT 機器の開発に関する次の記述を読んで，設問 1～3 に答えよ。

V 社は，IoT 機器を製造・販売している従業員数 3,000 名の会社である。家庭用ゲーム機（以下，ゲーム機 V という）の発売を予定しており，設計を開発部が担当している。設計リーダは，開発部の H さんである。利用者はゲーム機 V とゲームプログラムの利用権を購入し，ゲーム機 V からゲームサーバ上のゲームプログラムを利用する。複数のゲームプログラム開発会社が，それぞれ複数のゲームプログラムを開発し，販売する予定である。開発部が設計したゲーム機 V，認証サーバ及びゲームサーバ（以下，三つを併せてゲームシステム V という）の構成を図 1 に，構成要素とその概要を表 1 に示す。



注記 1　ファイアウォールなどのネットワーク機器は省略している。
注記 2　ゲーム機 V と各サーバとの間の通信には，HTTP over TLS を使用する。
注 1)　利用者 ID，パスワードのハッシュ値，ニックネーム，性別及び誕生日から成る。
2)　利用者 ID，利用者が購入したゲームプログラムのゲームプログラム ID から成る。

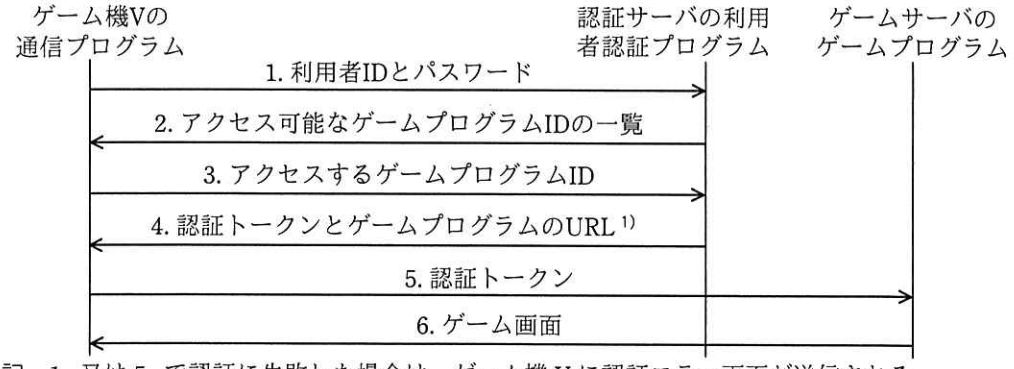
図 1　ゲームシステム V の構成（概要）

表1　ゲームシステムVの構成要素とその概要

構成要素	概要
ゲーム機V	・無線LAN機能，コントローラ[1]及びディスプレイを備えている。 ・専用OSがインストールされており，ブートローダから起動される。 ・専用 OS に含まれる通信プログラムは，ゲームサーバ上のゲームプログラム及び認証サーバ上の利用者認証プログラムと通信する。 ・通信プログラムは，コントローラの操作情報をリアルタイムにゲームプログラムに送信し，ゲームプログラムからゲームの処理結果をゲーム画面として受信してディスプレイに表示する。 ・ゲーム機Vごとに一意のデバイスIDが付与される。 ・ゲーム機Vごとに発行されたクライアント証明書を格納している。各サーバとの通信時には，クライアント証明書を使用したクライアント認証が行われる。 ・各サーバとの通信時には，サーバ認証を行い，クラウドV中のサーバとだけ通信を行う。 ・初期セットアップ時に認証サーバに利用者情報を登録する。 ・PC に接続しても外部ストレージとして認識されず，内部のデータを直接読み出すことはできない。
ゲームサーバ	・クラウド V に複数のゲームプログラム開発会社がそれぞれゲームサーバを立ち上げ，各ゲームサーバで一つ又は複数のゲームプログラムを稼働させる。 ・ゲームプログラム開発会社のゲームサーバ管理者が運用する。 ・各ゲームプログラムには，固有のゲームプログラムIDが付与される。 ・ゲームサーバごとに発行されたサーバ証明書を格納している。
認証サーバ	・利用者情報と購入情報を管理する。 ・利用者認証プログラムは，ゲーム機 V がゲームプログラムを利用する際の利用者の認証を行う。認証の結果，利用者が購入したゲームプログラムだけの利用を許可する。 ・認証サーバに発行されたサーバ証明書を格納している。

注[1]　ゲームを行う際などに使用する入力装置

ゲームを行う際は図2の認証フローで利用者の認証が行われる。



注記　1. 又は5. で認証に失敗した場合は，ゲーム機Vに認証エラー画面が送信される。
注[1]　URLはゲームプログラムごとに固有である。

図2　利用者がゲームを行う際の認証フロー

認証トークンには，認証サーバの FQDN，利用者 ID 及び MAC（Message Authentication Code）が格納される。①MAC は，認証サーバの FQDN と利用者 ID に対して，ハッシュ関数を共通鍵と組み合わせて使用し，生成する。共通鍵は，ゲームシステム V 全体で一つの鍵が使用され，ゲームサーバ管理者がゲームプログラムに設定する。図 2 の 5. では，ゲームプログラムによる認証トークンの MAC の検証が成功し，かつ，FQDN が確かに認証サーバのものであることが確認された場合だけ，認証が成功し，図 2 の 6. でゲームプログラムからゲーム画面が送信される。

〔セキュリティレビューの実施〕

認証トークンが認証サーバ以外で不正に生成されると，購入していないゲームプログラムを利用されたり，クラウド V 上のリソースを不正に利用されたりするおそれがある。そこで仮に認証サーバ以外で認証トークンを生成されたとしてもゲームプログラムでは検証に失敗することが求められる。また，利用者がコントローラの不正な操作情報をゲーム機 V から送信することによって，ゲームを有利に進めるといったことも防ぐ必要がある。

V 社では，システム設計にセキュリティ上の問題がないか，製品の設計工程でセキュリティレビュー（以下，レビューという）を実施することになっており，ゲームシステム V はセキュリティ部の N さんがレビューを担当することになった。次は，N さんがゲームシステム V のレビューを行った時の，H さんとの会話である。

N さん：現状の認証トークンの設計には二つの問題があります。一つ目の問題は，現在の設計では認証トークンに格納される情報が不足しているということです。情報が不足していることによって，ゲームプログラム A 用の認証トークンがゲームプログラム B においても認証に成功してしまうので，攻撃者がゲームプログラムの URL を知ることができれば，購入していないゲームプログラムも利用できてしまいます。②この問題への対策を検討してください。

H さん：分かりました。

N さん：二つ目の問題は，③認証トークンをゲームサーバ管理者が不正に生成できてしまうことです。

H さん：その問題への対策としては，ゲームプログラムごとに別の共通鍵を利用するという設計はどうでしょうか。

N さん：それでは対策として不十分です。④その設計にしたとしても，不正にゲームプログラムが利用できる認証トークンをゲームサーバ管理者が生成できてしまいます。

H さん：MAC ではなく，ディジタル署名を利用すれば対策になりますか。

N さん：はい。そうすればゲームサーバ管理者が認証トークンを不正に生成したとしても，ゲームプログラムで検証が失敗します。

H さん：では，[a] で公開鍵と秘密鍵の鍵ペアを生成し，[b] をゲームサーバに配布しておきます。[a] が [c] を使って認証トークンに署名を付加し，ゲームプログラムでは [b] を使って署名の検証を行います。

N さん：それで問題ありません。次に，不正な機器から認証サーバとゲームサーバへのアクセスをどのようにして防ぐのか教えてください。

H さん：クライアント認証を使います。

N さん：ゲーム機 V 内のクライアント証明書とそれに対応する秘密鍵（以下，鍵 C という）が攻撃者の PC から不正に使用できると，その PC から各サーバに接続されてしまいます。さらに，コントローラの操作情報を改ざんして送信することによって，ゲームを有利に進めることも考えられます。クライアント証明書と鍵 C はゲーム機 V のどこに格納しますか。

H さん：鍵 C を含めた全てのデータは，搭載する SSD（Solid State Drive）に格納します。搭載する SSD は，広く流通しているものです。

N さん：それでは問題がありますね。現状の設計では，専用 OS に脆弱（ぜい）性が存在しなかったとしても，⑤攻撃者がゲーム機 V を購入すれば，専用 OS を改ざんせずに，ゲーム機 V 内のクライアント証明書と鍵 C を PC などから不正に使用できます。

H さん：どのように対策したらいいでしょうか。

N さん：TPM（Trusted Platform Module）をゲーム機 V に搭載し，TPM 内に鍵 C を保存するという方法があります。TPM は，⑥内部構造や内部データを解析されにくい性質を備えているので，TPM 内に鍵 C を保存すれば不正に読み

取ることは困難になります。

また，ブートローダ又は専用 OS の改ざんはゲーム機 V の不正利用につながります。例えば，コントローラの不正な操作情報を送信されるおそれがあります。そのため，ブートローダ及び専用 OS の改ざん対策についても検討してください。

H さん：分かりました。設計を見直します。

〔ブートローダ及び専用 OS の改ざん対策〕

2 回目のレビューでは，ブートローダ及び専用 OS の改ざん対策について確認した。次は，その時の H さんと N さんの会話である。

H さん：ブートローダ及び専用 OS の改ざんに備えた対策として，ブートローダ又は専用 OS が改ざんされていると判定されたときは，ゲーム機 V の起動処理を中止するようにしました。ブートローダ及び専用 OS の改ざん対策の処理の流れを図 3 に示します。

1. ブートローダ及び専用 OS 中の起動時に実行されるファイルのハッシュ値をあらかじめ計算し，ハッシュ値のリスト（以下，ハッシュ値リストという）を作成しておく。ゲーム機 V への専用 OS の導入時，ハッシュ値リストを併せて保存する。起動時に専用 OS 中のファイルが実行される順番は，あらかじめ決められている。
2. ゲーム機 V の起動時には，CRTM（Core Root of Trust for Measurement）と呼ばれる，改ざんが困難な起動コードから起動処理を開始する。
3. CRTM は，ブートローダのハッシュ値を計算し，そのハッシュ値がハッシュ値リスト中に存在することを確認できたら実行する。
4. ブートローダは，専用 OS の最初に実行されるファイルのハッシュ値を計算し，ハッシュ値リスト中に存在することを確認し，実行する。同様に，後続のファイルについて計算，確認，実行を繰り返し，専用 OS が起動する。
5. ハッシュ値がハッシュ値リスト中に存在しないファイルは改ざんされていると判定され，起動処理が中止される。

図 3　ブートローダ及び専用 OS の改ざん対策の処理の流れ

N さん：処理の流れは分かりました。ハッシュ値リストが保護されていないと，改ざんされたファイルが実行されるおそれがありますが，どのように対策していますか。

Hさんは，⑦ハッシュ値リストを保護するための方法を説明した。

Nさん：それであれば，改ざんされたファイルが実行される危険性は低いですね。

その後，クラウドVの準備が整い，ゲーム機Vが発売された。

設問1　本文中の下線①に該当する方式はどれか。該当する方式を解答群の中から選び，記号で答えよ。

解答群

ア　CBC-MAC	イ　CMAC	ウ　CSR
エ　HMAC	オ　MD5	カ　RC4

設問2　〔セキュリティレビューの実施〕について，(1)～(6)に答えよ。

(1)　本文中の下線②について，対策として認証トークンに追加する必要がある情報を，15字以内で答えよ。

(2)　本文中の下線③について，その原因となるゲームサーバの仕様を，30字以内で述べよ。

(3)　本文中の下線④について，その原因となる認証トークンの仕様を，20字以内で述べよ。また，不正に生成した認証トークンで利用できるゲームプログラムの範囲を，35字以内で述べよ。

(4)　本文中の［　a　］～［　c　］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　共通鍵	イ　ゲーム機V	ウ　ゲームサーバ
エ　公開鍵	オ　認証サーバ	カ　秘密鍵

(5)　本文中の下線⑤について，どのようにするとクライアント証明書と鍵Cを PC などから使用可能にしてしまうことができるか。攻撃者が使用前に行う必要があることを，25字以内で具体的に述べよ。

(6)　本文中の下線⑥について，この性質を何というか。10字以内で答えよ。

設問3　本文中の下線⑦について，保護するための適切な方法を本文中の用語を使って，25字以内で具体的に述べよ。