■設問 3

［試験センターによる解答例］

(1) セキュリティ検査を本番システムに対し行うこと（22 字）

(2) ブラウザによっては XSS 攻撃を遮断する機能をもつから（26 字）

(3) W システムで当該脆弱性に対処する前に始まる攻撃によって，セキュリティ侵害されてしまうリスク（45 字）

(1) 問題文の〔W システムの実装に関する脆弱性〕にあるように，今回指摘された脆弱性は検査すべき項目の中に含まれており，開発用 PC 上のコードでは修正済みであったが，F 氏が本番システムに修正版をデプロイし忘れていたため，本番システムに脆弱性が残存したままとなっていた。このような問題を防ぐためには，本番システムに対してもセキュリティ検査を実施するよう手順を見直すのが有効である。

(2) Internet Explorer, Edge, Google Chrome, Safari など，一部のブラウザには XSS フィルタと呼ばれる XSS 攻撃の遮断機能が実装されている。そのため，K 氏によるブラウザを用いた検査では XSS 攻撃の試みを完遂できないことがある。

(3) 問題文の〔脆弱性対策の強化〕にあるように，S サービスでは，Web システムに脆弱性が発見された際，短時間で適切なシグネチャが WAF に追加される。このサービスを利用していれば，W システムで脆弱性が発見され，当該脆弱性に対処する前に始まる攻撃によってセキュリティ侵害されてしまうリスクを低減することができる。

＜問 3＞ SSL/TLS を用いたサーバの設定と運用

■設問 1

［試験センターによる解答例］

(1) a：コ
b：カ
c：オ
d：イ

(2) 正規の EC サイトの URL でアクセスしたときに，偽の EC サイトに誘導する。(36 字)

(3) エ

(1)

a：サーバ証明書の作成とその検証に利用しており，公開鍵暗号方式を使用した技術であるから，解答群で該当するのは「ディジタル署名」である。

b：SSL/TLS で，データの送受信時に暗号化と復号のために利用するのは「共通鍵暗号」である。

c：データの送信者と受信者が共通鍵暗号で使用する鍵を共有するために，公開鍵暗号方式を用いて行うのは「鍵交換」である。

d：サーバ証明書としてドメイン証明書とともに広く使用されているのは「EV 証明書」である。**EV（Extended Validation）証明書**とは，従来のディジタル証明書よりも，発行にあたっての審査基準を厳しく設定しており，組織が法的かつ物理的に実在することや，その組織が証明書に記載されるドメインの所有者であることが求められる。

(2) DNS キャッシュポイズニング攻撃は，DNS のキャッシュに偽の名前解決情報を登録することで，利用者を不正なサイトに誘導する手法である。攻撃者は，C 社の EC サイトを複製した偽の EC サイトを立ち上げた後，DNS キャッシュポイズニング攻撃で偽の名前解決情報を DNS キャッシュサーバに登録することにより，利用者が正規の EC サイトの URL でアクセスしたときに偽の EC サイトに誘導する。

(3) 擬似乱数生成器が生成する擬似乱数に規則性があったり，特定の文字が出現しやすかったり，同じ文字列が生成されるまでの周期が短かったりすれば，攻撃者によって推測される可能性が高まる。擬似乱数には予測不可能であることが求められる。

■設問 2

［試験センターによる解答例］

(1) ア：利用（2 字）
　　イ：失効（2 字）

(2)・鍵が危たい化した Web サイトの FQDN（19 字）
　　・鍵が危たい化したと思われる日時（15 字）

(3) g：鍵ペア（3 字）

(1) サーバ証明書に対する秘密鍵が危たい化した場合には，当該サーバ証明書の利用を停止するとともに，発行元に対して失効申請を行う必要がある。サーバ証明書等の失効情報は CRL（Certificate Revocation List）に登録される。CRL は有効期限内に失効させる必要が生じたサーバ証明書等が登録されたリストであり，認証局（CA）から随時発行される。

(2) 問題文の〔社外からの通報〕で H 氏が説明しているように，サーバ証明書にはサーバの FQDN と公開鍵が記載されている。サーバの利用者が自身の被害の可能性を判断できるようにするためには，まず鍵が危たい化した Web サイトの FQDN を公表する必要がある。また，鍵の危たい化が発生したと思われる日時を公表することも重要である。

(3) 秘密鍵が危たい化した場合に，システムを復旧させるには，鍵ペアを生成した上で，生成した新たな公開鍵が記載されたサーバ証明書の発行を受ける必要がある。

■設問 3

［試験センターによる解答例］

(1) SSL3.0 を利用しない設定にする。(18 字)

(2) ウ，オ

(3) エ

(4) ドメイン認証証明書ではサーバの運営者が C 社であることを確認できないから (35 字)

(1) 図 4 の POODLE 攻撃の概要に「SSL3.0 プロトコルのパディングチェックの脆弱性を利用した攻撃であり，ソフトウェアの開発時に起こり得る実装上のミスによる脆弱性を利用するものではない」とあることから，SSL3.0 のプロトコルに問題があることがわかる。また，TLS1.0 以降のプロトコルについては「攻撃の可能性はあるが，実装上の問題がなければ成功は困難と考えられている」とある。これらのことから，各サーバに SSL3.0 を利用しない設定を施すことで，POODLE 攻撃を受ける脆弱性に対処することが可能と判断できる。

(2) PFS とは，暗号化されたデータと秘密鍵が漏えいした場合であっても，過去の暗号データを復号することが不可能であるという性質であり，前方秘匿性と訳される。解答群の中でこれに該当するのは，DHE（Ephemeral Diffie-Hellman）と ECDHE（Elliptic Curve Diffie-Hellman Exchange）である。

(3) RSA の鍵が危たい化したことにより，攻撃者はセッション鍵を共有するための秘密情報を復号し，そこからセッション鍵を取得することが可能となる。これにより，攻撃者によって取得された危たい化前後における通信データを全て復号されてしまうおそれがある。

(4) 前述のように，EV 証明書の場合，発行に際に組織が法的かつ物理的に実在することや，その組織が証明書に記載されるドメインの所有者であることが求められる。一方ドメイン認証証明書では，発行の際にドメインの所有名義について確認するのみで，組織の実在性については確認しない。そのため，サイトの利用者はサーバの運営者が C 社であることを確認することができないことになり，新たに立ち上げた EC サイトが使用するサーバ証明書として適切とはいえない。