問3　SSL/TLS を用いたサーバの設定と運用に関する次の記述を読んで，設問 1～3 に答えよ。

C 社は，衣服のデザイン，製造及び販売を行う中堅の衣料品製造会社である。近年は，C 社の複数の販売チャネルのうち，EC モールに出店したオンラインショップでの販売量が増えており，C 社の社名も比較的知られるようになった。C 社では，事業を更に拡大するために，新たに独自のドメイン名を取得し，C 社専用の販売サイト（以下，EC サイトという）を立ち上げることにした。

EC サイトの構築，運用及び管理は，C 社のシステム部が担当することになった。システム部は開発会社の協力を得て構築を進め，当初の計画どおり運用が開始された。

〔社外からの通報〕

運用開始から 3 か月が経過した頃，C 社の問合せ窓口に，EC サイトで利用されている一部のサーバ証明書に対応する秘密鍵が，サーバ証明書と一緒に，ある Web サイト（以下，Q サイトという）に掲示されているという通報があった。そこで，システム部の M 部長は，EC サイトの管理を担当する B さんに，セキュリティ専門会社である E 社の支援を得て本件を調査し必要な措置を講じるよう指示した。

E 社のセキュリティコンサルタントである H 氏のアドバイスを受けて B さんが確かめたところ，Q サイトに掲示された秘密鍵は自社のものと一致していた。B さんは鍵が危たい化したと判断した。

次は，H 氏と B さんの会話である。

H 氏　：サーバ証明書に対応する秘密鍵が公開された影響について，順に説明していきましょう。サーバ証明書は認証局サービス事業者から発行されます。サーバ証明書には，サーバの FQDN と公開鍵が記載されます。サーバ証明書の作成とその検証には公開鍵暗号方式を利用した［　a　］技術を利用します。サーバ証明書は SSL/TLS で利用されます。SSL/TLS は複数の暗号技術を用います。データの送受信時は，暗号化と復号のために［　b　］を利用します。また，データの送信者と受信者が［　b　］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［　c　］を行います。現在，世の中で発行されているサーバ証明書には複数の種類があり，代表的なものはドメイン認証証明書と［　d　］です。サーバ証明書の種類によって，認証局サービス事業者が発行時に行う審査の内容が異なります。

秘密鍵を知った者は，御社の EC サイトと利用者との通信パケットを入手できれば，それを復号して内容をのぞき見できる可能性があります。また，御社の EC サイトを複製して偽の EC サイトを立ち上げ，①DNS キャッシュポイズニング攻撃と組み合わせて，不正を行うかもしれません。

H 氏は，DNS キャッシュポイズニング攻撃について説明した。

B さん：分かりました。でも，なぜ鍵が他者に知られてしまったのでしょうか。

H 氏　：経緯はまだ分かりません。Q サイトには，サーバ証明書のうち，ある古い暗号ソフトウェア（以下，Z ソフトという）を用いて鍵ペアが生成されたものを対象に秘密鍵の推定を試み，推定に成功したものを掲示している旨の説明がありました。御社は Z ソフトを利用していませんか。②鍵ペアの生成に用いる擬似乱数生成器に必要な条件を，Z ソフトは，満たさないことが分かっています。

〔鍵の危たい化への初動対応〕

H 氏は，次の二つの措置をとるように B さんにアドバイスした。

・当該鍵に関わるサーバ証明書の［　ア　］停止

・当該鍵に関わるサーバ証明書の［　イ　］申請

H 氏は，今後，再び鍵の危たい化が起きた場合に備えて，あらかじめ検討して準備しておくことが望ましい事項について，B さんに説明した。その事項を図 1 に示す。

・鍵の危たい化に対応するための体制，及びその役割と責任（認証局サービス事業者との連携を含む。）
・鍵が危たい化した又はそのおそれがあると判断する基準
・鍵が危たい化した又はそのおそれがあると判断した場合の実施事項
(1) 当該鍵に関わるサーバ証明書の［ア］停止
(2) 当該鍵に関わるサーバ証明書の［イ］申請
(3) 原因の調査
(4) 影響範囲の調査
(5) 原因の除去
(6) ③当該鍵を使用していたサーバの利用者が，自身の被害の可能性を判断できるようにするための情報の公表
(7) その他の必要な是正処置
・システムを復旧させる際の遵守事項
(1) 危たい化した鍵に関わる証明書署名要求（CSR）の再利用禁止
(2) ［e］の生成と，その利用

図1　あらかじめ検討して準備しておくことが望ましい事項

〔H氏による調査及び問題の指摘〕

Bさんは，秘密鍵が他者に知られてしまった原因と，SSL/TLSの利用に関してECサイトの設定などに改善すべき問題がないかについて，H氏に調査を依頼した。

H氏による調査の結果を図2に，暗号スイートの名前の構成を図3に示す。

1. ECサイトの設定など基本情報
・ECサイトのサーバ数：5台
・社外からアクセスできる全てのサーバでSSL/TLSを利用
利用可能なプロトコルのバージョン：SSL 3.0，TLS 1.0，TLS 1.1，TLS 1.2
・サーバの鍵ペアは，Zソフトを利用して生成
鍵ペアは，特定の機器で生成されていた。当該機器にZソフトがインストールされていた。
・SSL/TLSの暗号スイートに，次のものを設定
(1) TLS_RSA_WITH_AES_128_CBC_SHA
(2) TLS_RSA_WITH_AES_128_CBC_SHA256
(3) TLS_RSA_WITH_AES_128_GCM_SHA256
(4) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
(5) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
(6) TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
(省略)
・サーバ証明書は，認証局サービス事業者Y社が発行するドメイン認証証明書を採用
2. 秘密鍵が他者に知られてしまった原因
・鍵ペアの生成にZソフトを利用していたので，Qサイトが推定に成功したと推測
3. SSL/TLSの利用に関して改善すべき問題
問題1　POODLE攻撃に対して脆弱(ぜい)であること
問題2　Perfect Forward Secrecy（以下，PFSという）に対応していないこと
問題3　サーバ証明書にドメイン認証証明書を用いていること

図2　H氏による調査の結果（抜粋）

TLS_RSA_WITH_AES_128_CBC_SHA
(a) (b) (c)

(a) 認証及び鍵交換のアルゴリズム
(b) データ暗号化のアルゴリズム
(c) MAC又はPRF（Pseudorandom Function）のアルゴリズム

図3　暗号スイートの名前の構成（概要）

問題1中のPOODLE攻撃の概要を図4に示す。H氏は，④問題1を解決するために各サーバに施すべき措置を提案した。

・POODLE攻撃によって，攻撃者は，暗号化された通信データの一部を解読し，取得できる。
・中間者攻撃が可能であり，かつ，攻撃対象に大量のデータを送信できることなどの一定の条件を満たす場合に，攻撃が成功する。
・SSL 3.0 プロトコルのパディングチェックの脆弱性を利用して攻撃する。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。
・TLS 1.0 以降のプロトコルについて，同様のパディングチェックの仕組みを突いた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。

図4　POODLE攻撃の概要

問題2は，C社がSSL/TLSのハンドシェイクにおいて，⑤PFSの性質をもつ鍵交換方式を利用せず，代わりに，⑥セッション鍵を共有するための秘密情報をクライアントがサーバ証明書に記載されたRSAの公開鍵を用いて暗号化して送信する方式を用いていたことである。

問題3は，サーバ証明書の種類についてである。H氏は，⑦ECサイトが新たに立ち上げたサイトであることを考慮すると，ドメイン認証証明書の選択は妥当でないと指摘した。

〔対策実施と運用見直し〕

Bさんは，H氏の支援を受け，各問題について解決策を検討した。また，M部長の承認の下，図1の事項の検討も進めた。C社は，Qサイトに関わる通報を受けた1か月後には，各問題を解決し，今後起こり得る鍵の危たい化に備えた態勢を整えた。

設問1　〔社外からの通報〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］～［ d ］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　CA 証明書	イ　EV 証明書	ウ　エンコード方式
エ　エンティティ認証	オ　鍵交換	カ　共通鍵暗号
キ　公開鍵	ク　自己解凍	ケ　相互認証証明書
コ　ディジタル署名	サ　ハッシュ関数	シ　メッセージ認証
ス　ルート証明書		

(2) 本文中の下線①について，DNS キャッシュポイズニング攻撃は偽の EC サイトと組み合わせた不正の中でどのような役割を果たすか。40 字以内で具体的に述べよ。

(3) 本文中の下線②について，擬似乱数生成器が生成する乱数列に求められる性質として，適切なものを，解答群の中から選び，記号で答えよ。

解答群

ア　一様分布でない。	イ　規則性がある。
ウ　周期が短い。	エ　予測不可能である。

設問2　〔鍵の危たい化への初動対応〕について，(1)～(3)に答えよ。

(1) 本文中及び図 1 中の［ ア ］，［ イ ］に入れる適切な字句を，それぞれ5字以内で答えよ。

(2) 図 1 中の下線③について，公表すべき情報として，重要なものを二つ挙げ，それぞれ 20 字以内で具体的に述べよ。

(3) 図1中の［ e ］に入れる適切な字句を，7字以内で答えよ。

設問3　〔H 氏による調査及び問題の指摘〕について，(1)～(4)に答えよ。

(1) 本文中の下線④について，H 氏が提案した措置を，20 字以内で述べよ。

(2) 本文中の下線⑤について，SSL/TLS の利用において，PFS の性質をもつ鍵交換方式を解答群の中から全て選び，記号で答えよ。

解答群

ア　AES	イ　CFB	ウ　DHE	エ　DSA
オ　ECDHE	カ　ECDSA	キ　PKCS	ク　RSA

(3) 本文中の下線⑥について，RSA の鍵が危たい化した場合に，当該鍵を用いてハンドシェイクを行った通信に関するリスクは何か。そのリスクの説明として，最も適切なものを解答群の中から選び，記号で答えよ。ここで，攻撃者は，Web ブラウザと Web サーバの通信経路上におり，危たい化前後における通信データを取得していたものとする。

解答群

ア 取得された通信データのうち，鍵が危たい化した時点より前の通信データだけを，復元されるおそれがある。

イ 取得された通信データのうち，鍵が危たい化した時点で通信中だった通信データだけを，復元されるおそれがある。

ウ 取得された通信データのうち，鍵が危たい化した時点より後の通信データだけを，復元されるおそれがある。

エ 取得された通信データの全てを復元されるおそれがある。

(4) 本文中の下線⑦について，妥当でないと指摘した理由を，40 字以内で述べよ。