問2　代理店販売支援システムに関する次の記述を読んで，設問1～3に答えよ。

L社は中堅の損害保険会社である。保険商品は，直営店でも扱っているが，多くは代理店を通じて販売している。L社では，10年前にインターネットを用いた代理店販売支援システム（以下，Pシステムという）を開設した。

Pシステムは，代理店に対して，顧客情報の新規登録，閲覧及び更新の機能，並びに商品説明書及び販売マニュアルの提示機能を提供する。代理店の担当者は，利用者IDとパスワードを入力してログインし，Pシステムを利用する。

Pシステムの開設以来，Pシステムへの不正ログインの試みと推測される事象が複数回確認されてきた。また，3年前には，競合他社において代理店から大量の顧客情報が流出する事件も発生した。これらの状況において，L社は代理店に対して，注意喚起，講習会の開催，年1回のセキュリティチェックレポート提出の要請などを実施してきた。

運用開始から10年目を迎えることを機に，L社では，Pシステムを全面改修・拡張して，新システム（以下，Qシステムという）を構築することにした。そのプロジェクトのリーダには，IT部門のB課長が任命された。プロジェクトの重要な目的の一つは，セキュリティの強化である。Qシステムのセキュリティ設計は，B課長の部下であるCさんが担当することになった。

〔Qシステムの設計方針〕

Qシステムは，Pシステムを拡張して構築する。2015年9月から10年間の稼働を想定している。Qシステムには，情報漏えいのリスクをできるだけ減らすことが求められている。B課長は，経営陣，代理店チャネル担当，情報セキュリティ室などの社内関係者及び社外の情報セキュリティの専門家に意見を求め，表1に示す情報漏えい防止設計方針を取りまとめた。

表１　情報漏えい防止設計方針（抜粋）

情報漏えい対策	設計方針
利用者の認証	・利用者 ID とパスワードだけでなく，多段階又は複数要素で利用者を認証することによって，なりすましによる不正アクセスを防止する。
端末の限定	・代理店の管轄下にある端末からのアクセスだけを許可する。
ガイドラインの作成	・顧客情報の取扱いや Q システムの利用要件についてガイドラインを作成し，その遵守義務を代理店契約に盛り込む。

C さんは，表１の設計方針のうち，利用者の認証及び端末の限定についての実現方法として，Q システムへのアクセス時に，従来の利用者 ID とパスワードでの認証に加え，SSL クライアント認証を行う方法を提案した。SSL クライアント認証では，あらかじめディジタル証明書（以下，証明書という）を代理店の端末に配布しておき，その証明書を用いた認証によって端末の限定を行う。

B 課長は，C さんが提案した方法について説明を受け，了承した。その上で，暗号技術について，情報セキュリティ室の R 主任に相談するよう助言した。

〔暗号技術の検討〕

次は，C さんが暗号技術について R 主任に相談したときの会話の一部である。

C さん：Q システムで使う暗号技術について，どのように検討を進めるのがよいでしょうか。

R 主任：SSL クライアント認証の場合には，まず，認証に使う公開鍵の鍵長，証明書に施されるディジタル署名の仕様，それから，通信の暗号化に使う共通鍵暗号の仕様などを選択する必要があるね。

C さん：何を基準にして選択すればよいのですか。

R 主任：表 2 は，米国国立標準技術研究所（NIST）が発行したセキュリティ文書を基に，攻撃の困難性の視点から，暗号アルゴリズムの安全性を整理したものだ。最も効率が良い攻撃手法で暗号を解読するときに必要な計算量を指標とし，同程度の耐性をもつものを同じ“セキュリティ強度”としている。また，“利用終了時期の目安”の行は，そのセキュリティ強度の暗号アルゴリズムについて，利用を終了することが望ましい時期を示している。

C さん：なるほど。例えば，鍵長 256 ビットの AES アルゴリズムは，鍵長

[a] ビットの RSA アルゴリズムや，[b] ビットのハッシュ関数などと同じセキュリティ強度ということですか。Q システムの場合は，少なくとも [c] ビット安全性と同等又はそれ以上のセキュリティ強度をもつ暗号アルゴリズムを採用すべきですね。頂いたアドバイスを参考に，更に検討します。

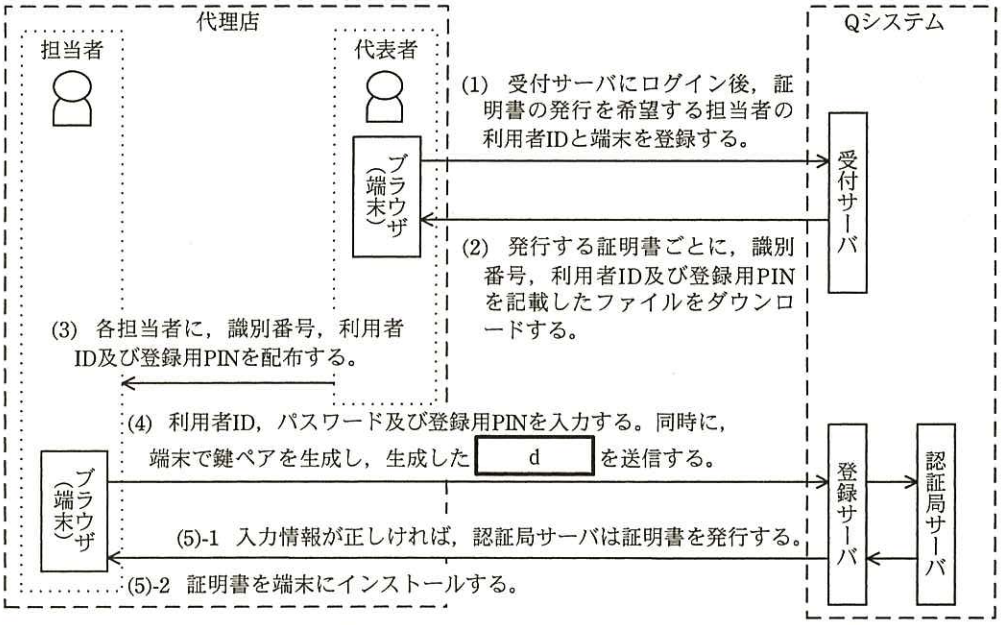
表 2　暗号アルゴリズムの安全性

項目 ＼ セキュリティ強度		80 ビット安全性	112 ビット安全性	128 ビット安全性	192 ビット安全性	256 ビット安全性
共通鍵暗号		80	112	128	192	256
公開鍵暗号	素因数分解問題に基づくアルゴリズム	1,024	2,048	3,072	7,680	15,360
	離散対数問題に基づくアルゴリズム	1,024	2,048	3,072	7,680	15,360
	楕(だ)円曲線上の離散対数問題に基づくアルゴリズム	160	224	256	384	512
ハッシュ関数		160	224	256	384	512
利用終了時期の目安		2013 年	2030 年	2031 年以降	2031 年以降	2031 年以降

注記 1　暗号の各行の数値は，鍵のビット数である。
注記 2　ハッシュ関数の行の数値は，ディジタル署名とハッシュ単独利用の場合におけるハッシュ値のビット数である。

〔Q システムのセキュリティ設計〕

C さんは，R 主任のアドバイスを参考に，Q システムのセキュリティ設計について検討を進めた。証明書の新規発行手順案を図 1 に，証明書についての補足情報を図 2 に示す。代理店に遵守を求めるガイドラインには，顧客情報の取扱要件に加え，①Q システムにアクセスしていた端末を交換及び廃棄する場合に代理店が実施すべき処理などの事項を盛り込んだ。



受付サーバ：Qシステムの窓口となるサーバであり，アクセスにはSSLクライアント認証を必須とする。
登録サーバ：証明書の発行受付のための専用サーバである。SSLクライアント認証はない。
認証局サーバ：証明書を発行するサーバである。
代表者：代理店が指定し，L社に登録する。代表者は，必要な証明書の発行をL社に申請する。代表者に与える最初の証明書は，別途定めた手順に従って発行する。
担当者：代理店においてQシステムを利用する者を示す。
識別番号：個々の証明書の発行及び更新ごとに付与する一意な番号である。証明書の管理のために利用する。

注記 証明書には，証明書のシリアル番号，利用者 ID，公開鍵，識別番号などを登録する。

図１　証明書の新規発行手順案

1. 証明書の利用停止手順

(1) 利用を停止する証明書の利用者である担当者が，受付サーバにログインし，利用を停止する証明書の [e] 又は識別番号を入力する。

(2) 受付サーバは，入力された情報で，ログインした担当者に発行された有効な証明書かを確認した後，当該証明書の識別番号を受付拒否リストと呼ばれるリストに登録する。

2. 証明書の更新手順

(1) 担当者は登録サーバにアクセスし，更新前の証明書と，当該秘密鍵の保持を示す署名データを提示する。

(2) 登録サーバは，提示された証明書と署名データを検証し，認証局サーバが発行した証明書であること，証明書に対応する秘密鍵を端末が保持していること，及び有効期間の終了まで 60 日以内であることを確認する。全て確認できれば，端末に対して新鍵ペアの生成を要求する。

(3) 認証局サーバは，新鍵ペアに対して新しい証明書を発行する。

図２　証明書についての補足情報

3. 受付サーバにおける担当者及び代表者のログイン処理時の検証項目（順不同）
- 入力された利用者 ID に対して，正しいパスワードが入力されたこと
- 提示された証明書が，認証局サーバが発行した証明書であること
- 証明書に対応する秘密鍵を，端末が保持していること
- 証明書の有効期間内であること
- 証明書中の識別番号が [f] に登録されていないこと
- [g] が，証明書中の [h] と一致すること

4. その他の補足事項
- 証明書の有効期間内に更新が行われなかった場合は，新規発行手順で対応する。
- 証明書に対応する秘密鍵は，端末から容易に抽出できないように設定する。

図 2　証明書についての補足情報（続き）

〔セキュリティ設計の修正〕

C さんは，セキュリティ設計の検討結果について R 主任にレビューを依頼した。R 主任は，証明書の新規発行手順，利用停止手順及び更新手順について一つずつ問題を指摘した。

R 主任は，証明書の新規発行手順については，代理店の担当者が不適切な行為をした場合，表 1 中の“端末の限定”の設計方針が満たされず，代理店の管轄下にない端末で Q システムにアクセスできる可能性があると指摘した。②この問題については，Q システムでは対策をとらず，代理店側で対策をとってもらうように，代理店に要請することにした。

R 主任は，証明書の利用停止手順については，実際には行うことができない場合が多いと推測されるので，見直さなければならないと指摘した。C さんは，この問題について，表 3 に示す修正案を考えた。検討の結果，設計方針への適合性と運用の柔軟性確保の視点から，案(2)を採用することにした。

表 3　証明書の利用停止手順の修正案

案	修正の概要	長所	短所
(1)	受付サーバへのログイン時に SSL クライアント認証を要求しない。	担当者本人による迅速な停止が期待できる場合がある。	情報漏えい防止設計方針と相違する部分がある。
(2)	役割と権限を見直し，[i]。	担当者が不在の場合にも，証明書の利用停止が可能である。	代表者の役割が拡大し，権限が集中する。

R 主任は，証明書の更新手順については，利用停止された証明書の取扱いを担当者が誤った場合などに，③本来発行されるべきでない証明書が発行される可能性があると指摘した。C さんは，この問題についても修正案を考えた。

C さんは，これらの修正案を基に図 1 及び図 2 の修正版を作成し，再度 R 主任のレビューを受けた後，B 課長に説明した。B 課長は修正版を了承し，Q システムの開発が進められることになった。

設問 1　〔暗号技術の検討〕について，(1)～(3)に答えよ。

(1)　本文中の [a]，[b] に入れる適切な数値を答えよ。

(2)　鍵長 3,072 ビットの RSA アルゴリズムと同等又はそれ以上のセキュリティ強度をもつと考えられるハッシュ関数を解答群の中から全て選び，記号で答えよ。

解答群

ア	Camellia	イ	ECDSA	ウ	MD5	エ	RC4
オ	SHA-1	カ	SHA-256	キ	SHA-512	ク	Triple DES

(3)　本文中の [c] に入れる適切な数値を答えよ。また，この数値は Q システムのどのような要件から導かれるか。20 字以内で述べよ。

設問 2　〔Q システムのセキュリティ設計〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，代理店が実施すべき処理を，30 字以内で具体的に述べよ。

(2)　図 1 中の [d] 及び図 2 中の [e] ～ [h] に入れる適切な字句を，図 1 又は図 2 中の字句を用いて，それぞれ 10 字以内で答えよ。

設問 3　〔セキュリティ設計の修正〕について，(1)～(3)に答えよ。

(1)　本文中の下線②について，代理店がとる対策を，40 字以内で具体的に述べよ。ここで，代理店の代表者は不適切な行為をしないものとする。

(2)　表 3 中の [i] に入れる適切な内容を 30 字以内で述べよ。

(3)　本文中の下線③のような証明書が発行されることを防ぐために，登録サーバにおける処理内容にどのような処理を追加すればよいか。40 字以内で述べよ。