次の問１は必須問題です。必ず解答してください。

問１　ファイルの安全な受渡しに関する次の記述を読んで，設問１～３に答えよ。

情報システム会社の X 社では，プロジェクトを遂行する際，協力会社との間で機密情報を含むファイルの受渡しを手渡しで行っていた。X 社は，効率化のために，次期プロジェクトからは，インターネットを経由してファイルを受け渡すことにした。

X社で働く A さんは，ファイルを受け渡す方式について検討するように，情報セキュリティリーダである E さんから指示された。A さんは，ファイルを圧縮し，圧縮したファイルを共通鍵暗号方式で暗号化した上で電子メール（以下，メールという）に添付して送信し，別のメールで復号用の鍵を送付する方式を E さんに提案した。しかし，E さんから“①A さんの方式は安全とはいえない”との指摘を受けた。

A さんは，暗号化について再検討し，圧縮したファイルを公開鍵暗号方式で暗号化してメールに添付する方式を E さんに提案したところ，“その方式で問題はないが，相手の［ a ］を入手する際には，それが相手のものであると確認できる方法で入手する必要がある点に注意するように”と言われた。

設問１　本文中の下線①で E さんから指摘を受けた理由として，最も適切な答えを，解答群の中から選べ。

解答群

ア　圧縮してから暗号化する方式は，暗号化してから圧縮する方式よりも解読が容易である。

イ　圧縮ファイルを暗号化してもファイル名は暗号化されない。

ウ　共通鍵暗号方式は，他の暗号方式よりも解読が容易である。

エ　ファイルを添付したメールと，鍵を送付するメールの両方が盗聴される可能性がある。

設問２　本文中の［　　］に入れる適切な答えを，解答群の中から選べ。

aに関する解答群

ア　共通鍵　　イ　公開鍵　　ウ　ディジタル署名

エ　パスワード　　オ　秘密鍵

設問３　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

次期プロジェクトでは，協力会社であるＰ社，Ｑ社，Ｒ社及びＳ社と協業する。プロジェクトの期間は 12 か月である。A さんは，各協力会社との間でファイルを受け渡す方式について，E さんから次のように指示されたので，更に検討を進めることにした。

〔ファイルを受け渡す方式に関するＥさんからの指示〕

(1)　メールを使用する方式以外も検討すること。

(2)　ファイルを受け渡す方式は，協力会社ごとに異なっていてもよい。

(3)　協力会社間ではファイルを受け渡さない。

(4)　ある協力会社との間で，ファイルを受け渡すためにアカウントを登録する必要があるシステムを使う場合，その会社からプロジェクトに参加する社員全員のアカウントを登録すること。

(5)　受け渡すファイルの機密度に合った方式を選択すること。機密度には“低”と“高”の２種類がある。X 社のセキュリティポリシでは，機密度が“高”のファイルを，オンラインストレージサービスを利用して受け渡すことを禁止している。

(6)　費用（初期費用とプロジェクト期間中の運用費用の合計）が最も安い方式を選択すること。

各協力会社の参加人数及び受け渡すファイルの機密度は，表１のとおりである。

表1　協力会社の参加人数及び受け渡すファイルの機密度

協力会社	参加人数（人）	受け渡すファイルの機密度
P社	10	“低”だけ
Q社	5	“低”と“高”
R社	50	“低”だけ
S社	25	“低”と“高”

Aさんは，ファイルを受け渡す方式として，次の三つの候補を検討した。

〔ファイルを受け渡す方式の候補〕

(1)　VPNとファイルサーバ

X社の拠点と協力会社の拠点との間でVPN環境を構築し，ファイルを受け渡すためのファイルサーバをX社に設置する。協力会社ごとに，異なるVPN環境の構築と異なるファイルサーバの設置を行う。この方式では，一つの協力会社につき，初期費用としてVPN環境の構築とファイルサーバの設置に100,000円，運用費用としてファイルサーバの運用及びVPN利用に，合わせて月額50,000円が掛かる。初期費用，運用費用ともに利用者数の多寡による影響はない。

(2)　オンラインストレージサービス

インターネット上で提供されているオンラインストレージサービスを利用してファイルを受け渡す。このサービスは，利用者にHTTP over TLSでのアクセスを提供しており，ファイルを安全に受け渡せる。この方式では，初期費用は掛からないが，運用費用として利用者1人当たり月額500円が掛かる。X社では，全社員がこのサービスを利用することにしたので，X社の社員についての運用費用はこのプロジェクトの費用には含めない。

(3)　暗号化機能付きメールソフト

公開鍵暗号方式を使った暗号化機能付きメールソフトを導入し，メールにファイルを添付して受け渡す。この方式を安全に運用するためには，導入時にプロジェクトの参加者全員に対して，メールソフトの利用方法などに関する研修が必要である。この方式では，初期費用として，メールソフトの導入及び研修

に，利用者 1 人当たり 30,000 円が掛かるが，運用費用は掛からない。X 社では，全社員がこのメールソフトを利用することにしたので，X 社の社員についての初期費用はこのプロジェクトの費用には含めない。

A さんは，各協力会社との間でファイルを受け渡す方式について，E さんからの指示に基づき協力会社ごとに選択すべき方式を検討した。その結果と，費用（初期費用とプロジェクト期間中の運用費用の合計）を，表 2 に示す。

表 2　選択すべき方式とその費用

協力会社	選択すべき方式	費用（円）
P 社	オンラインストレージサービス	60,000
Q 社	b	
R 社		
S 社	c	d

注記　網掛けの部分は表示していない。

b，c に関する解答群

ア　VPN とファイルサーバ

イ　オンラインストレージサービス

ウ　暗号化機能付きメールソフト

d に関する解答群

ア　30,000	イ　60,000	ウ　150,000
エ　300,000	オ　700,000	カ　750,000
キ　1,500,000		