平成29年春 情報セキュリティ ファイルの安全な受け渡し

問1　ファイルの安全な受渡し（情報セキュリティ）　(H29春-FE 午後問1)

【解答】

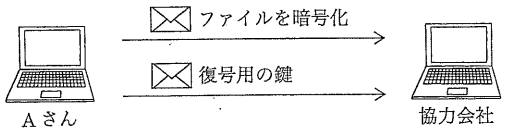
［設問1］　エ
［設問2］　a－イ
［設問3］　b－ウ，c－ア，d－オ

【解説】

複数の協力会社と協業して取り組むプロジェクトにおいて，各協力会社との間でのファイルの受渡しにおける安全な方式を選定することを題材にした問題である。また，設問五つのうち三つでは，複数の方式案の中から，E さんから提示された要件を満たす適切な方式を，費用面も考慮した上で選択する能力が問われている。難しい問題ではないが，問題文にある前提条件をしっかりと理解しないと解けない。公開鍵暗号方式に関する基本的な知識を前提にして，きちんと読み取れていれば解答できたであろう。

［設問1］

「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」理由が問われている。まず，A さんの方法を問題文から確認すると，「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」とある。



この方式については多くの企業が採用している方法である。と同時に，この方法には疑問を感じている人も多いため，選択肢を見る前に解答が想像できた人もいたのではないだろうか。(エ) の「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」が正解である。ファイルを添付したメールが盗聴できるのであれば，鍵を送付するメールも盗聴できるだろうし，両者が揃えば，暗号化したファイルが復号できてしまう。

他の選択肢も確認しておく。

ア：「圧縮してから暗号化する方式」も，「暗号化してから圧縮する方式」も，解読の難易の差はないと考えられる。しかし，先に暗号化してしまうと，圧縮に利用されるデータの中の繰返し部分やパターン部分がなくなってしまうことから圧縮効率が悪くなる。このため，一般に「圧縮してから暗号化する方式」が用いられる。

イ：ファイル名が暗号化されるかどうか，問題文では具体的には示されていないため，正解にならない。また，ファイル名が暗号化されるかどうかは，暗号化をするソフトウェアの仕様による。

ウ：同じ長さの鍵を前提にした場合，共通鍵暗号方式は，公開鍵暗号方式よりも強度が高く，解読は容易ではない。

［設問2］

空欄 a に入れる適切な答えを選ぶ。問題文の該当部分は，「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」とある。また，「その方式」とは，「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」である。したがって，公開鍵暗号方式で相手から入手するものが正解になる。公開鍵暗号方式では，相手の「公開鍵」（イ）を入手し，これを使ってファイルを暗号化する。ファイルを復号できるのは相手の秘密鍵だけなので，第三者に盗聴されても解読される心配がない。

［設問3］

協力会社ごとに選択すべき方式と，その費用が記載されている表2の空欄を埋める。問題文の前提条件をきちんと読み取る必要がある。

ここで，設問文，〔ファイルを受け渡す方式に関する E さんからの指示〕から重要な部分を次に抜き出す。

・プロジェクトの期間は 12 か月である。
　→1 年間を前提とした費用を計算が必要である。
・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。……(4)
　→表 1 にある参加人数の全員の費用を計算する必要がある。
・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。……(5)
　→表 1 から“高”のファイルがある Q 社と S 社では，オンライストレージサービスは利用できない。
・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。
　→全ての方式の費用を合計し，最も安い方法を選択する。

各方式の費用を検討するための情報は次のようになる。

費用＼方式	(1)VPN とファイルサーバ	(2)オンラインストレージサービス	(3)暗号化機能付きメールソフト
初期費用	100,000 円	－	1 人当たり 30,000 円
運用費用	月額 50,000 円 →1 年間で 600,000 円	1 人当たり月額 500 円 →1 年間で 6,000 円	－
備考	利用者数の多寡による影響はない。	“高”のファイルがある Q 社と S 社では利用できない。	－

これを基に，各社の年間費用を整理すると次のようになる。網掛け部分が，協力会社ごとの最も安い方式である。

協力会社＼方式	(1)VPN とファイルサーバ	(2)オンラインストレージサービス	(3)暗号化機能付きメールソフト
P 社（10 人）	100,000＋600,000＝700,000	6,000×10＝60,000	30,000×10＝300,000
Q 社（5 人）	100,000＋600,000＝700,000	利用不可	30,000×5＝150,000
R 社（50 人）	100,000＋600,000＝700,000	6,000×50＝300,000	30,000×50＝1500,000
S 社（25 人）	100,000＋600,000＝700,000	利用不可	30,000×25＝750,000

・空欄 b，c，d：表のとおり，Q 社の選択すべき方式は「暗号化機能付きメールソフト」，S 社の選択すべき方式は，「VPN とファイルサーバ」，その費用は「700,000」である。したがって，空欄 b には（ウ），空欄 c には（ア），空欄 d には（オ）が入る。