ト）

これを 1 時間（3,600 秒），かつ 70%の回線使用率で処理するための回線速度は次のようになる。

$$\frac{1{,}200{,}000}{3{,}600 \times 0.7} \fallingdotseq \textbf{476M ビット／秒}$$

(2)〔パフォーマンス検証〕に「海外支店 X については例外的に，TC 端末に移行せずに，……」とあることから，TC サーバであるイ，エ，カは不要である。それを前提として，図 5 の A 社データセンタの DMZ と海外支店 X の DMZ の構成要素を比較すればよい。海外支店 X において他の支店と同等の技術的対策を行うには，解答群のそれ以外の構成要素（**ア**，**ウ**，**オ**，**キ**，**ク**）はいずれも必要である。

■設問 5

〔試験センターによる解答例〕

セキュリティ管理の状況を客観的に監査できないという不具合（28 字）

経済産業省が発行している「システム監査基準」に「システム監査人は，システム監査を客観的に実施するために，監査対象から独立していなければならない」とあるように，客観的な監査を行うため，監査人は監査対象から独立していること原則である。セキュリティ管理と監査の役割を一つの組織にもたせた場合，監査人の独立性が確保できず，**セキュリティ管理の状況を客観的に監査できなくなってしまう。**

＜問 2＞ データの取扱い

■設問 1

〔試験センターによる解答例〕

(1)マルウェア感染ファイルが複数の利用者の同期用フォルダ間で自動同期される。（36 字）

(2)マルウェア感染ファイルの発見時に利用者に警告を発する機能（28 字）

(1)表 2 の「同期機能」の説明にあるように，同期アプリによって利用者の PC ローカルディスク上に同期用フォルダを作成される。同期用フォルダには利用者のアカウントのルー

トフォルダと，当該利用者がアクセス権をもつ他の利用者のファイル及びフォルダの複製が作成され，これらは Q サービス上のそれぞれのフォルダ又はファイルと自動的に同期される。Q サービスの試験導入では，マルウェアに感染したファイルを Q サービスに登録した結果，同ファイルにアクセス権をもつ**複数の利用者の PC の同期アプリが，感染ファイルを自動的に同期用フォルダにコピーすることで拡散した**。下線①は，これを想定した措置である。

(2)試験導入期間において表出した問題として，委託先のクリエイタが，PC で編集していたファイルがマルウェアに感染したことに気付かずに，そのまま Q サービスに登録してしまったことで，複数の利用者に拡散した点が挙げられる。同期用 FS により，マルウェアが検知された場合には，Q サービス利用者フォルダや同期ディスクにある感染ファイルは削除されるが，そのことを利用者に通知する機能がない。そのため，利用者がマルウェア感染に気付かず，利用者 PC 上にある感染ファイルをメール等で拡散させてしまう可能性がある。こうした事態を防ぐため，同期用 FS には，**マルウェア感染ファイルの発見時に利用者に警告を発する機能**を追加すべきである。

■設問２

〔試験センターによる解答例〕

(1)a：ク

d：ア

e：オ

f：キ

(2)b：営業秘密（4 字）

c：公然と知られていない（10 字）

(1)

a：M 部長が三つの要件として，「当該データが，秘密として管理されていること，有用な情報であること，……」と説明していることから，該当するのは**ク**の「不正競争防止法」である。

d：窃盗罪が規定されている法律であるから，該当するのは**ア**の「刑法」である。

e：思想又は感情を創作的に表現したと考えられるデータが保護の対象となる法律であるから，該当するのは**オ**の「著作権法」である。

f：ネットワークを通じてサーバなどの電子計算機に対して行われる攻撃が対象であり，攻撃対象の機器を直接操作するケースは対象外となる法律であるから，該当するのは**キ**の「不正アクセス禁止法」である。

(2)

b：不正競争防止法では，M 部長が説明している三つの要件を満たす情報を保護の対象としており，「**営業秘密**」と定義している。

c：不正競争防止法が営業秘密の要件としているのは次の三つであり，該当するのは「**公然と知られていない**」である。

・秘密として管理されていること（秘密性）
　営業秘密であることが客観的に認識できるような管理がされている必要がある。
・技術上／営業上の有用な情報であること（有用性）
　経済効果をもたらす有用な情報であることが客観的に認識できる必要がある。
・公然と知られていないこと（非公知性）
　業界常識であったり，雑誌やホームページなどに掲載されたりしていないこと（既知となっていないこと）が求められる。

■設問３

〔試験センターによる解答例〕

(1)g：OS（2 字）

**　h：暗号化（3 字）**

(2)平文が同じブロックは同じ暗号文になるので，暗号文から平文を推測されやすい。（37 字）

(3)i：1

**　j：24**

**　k：1**

**　l：1**

**　m：5**

(4)n：CBC モード

**　o：OFB モード**

(1)

g : フルディスク暗号化方式では，PC の全ディスクが暗号化される。そのため，パスワードがないと **OS** を起動することができない。OS 起動後は，データの保護は PC の OS が提供する機能に委ねられる。

h : 仮想ディスク暗号化方式では，データは暗号化された上でコンテナ内に保管される。一方，スワップ領域やハイバネーション用ファイルに存在するデータであり，「保護されない」のであるから，［ h ］には「**暗号化**」が該当する。

(2)図 6 のように，ECB（Electronic Code Book）モードは，暗号ブロック間の関連性がなく，単に平文をブロックごとに区切り，暗号化する方式である。各ブロックが独立しているため，並列処理が可能で高速だが，**平文が同じブロックは同じ暗号文になり，暗号文から平文を推測されやすい**という問題がある。

(3)

i : 前述のように，ECB モードは暗号ブロック間の関連性がなく，各ブロックが独立しているため，修正したブロックに対して暗号化処理を実行すればよい。修正したのは 1 ブロック分であるため，暗号化処理の実行回数は **1 回**である。

j : 図 6 のように，CBC（Cipher Block Chaining）モードは，一つ前の平文ブロックの暗号化処理結果（暗号ブロック）と次の平文ブロックを XOR 演算し，その結果を暗号化する方式である。暗号化処理結果が次のブロックの入力値となるため，1,025 ビット目から始まる 1 ブロック分のデータを修正した場合には，そのブロック以降の全てのブロックで暗号化処理を実行する必要がある。512 バイトをビットに換算すると 4,096 ビットであり，このうち，1,024 ビットまでの 8 ブロック分については暗号化処理は不要である。残る 3,072 ビットについて暗号化処理が必要であり，その回数は 3,072 ÷ 128 ＝ **24 回**である。

k : ECB モードは各ブロックが独立しているため，1 ブロック分のデータを復号する場合も暗号化の逆処理を **1 回**実行すればよい。

l : CBC モードで 2 ブロック目以降のブロックを復号する場合には，対象となる暗号文 1 ブロックに対して暗号化の逆処理を実行した後，一つ前の暗号文 1 ブロックを入力値として XOR 演算を行うことで復号することができる。したがって，実行する暗号化の逆処理の回数は **1 回**である。

m : 図 6 のように，OFB（Output Feedback）モードは，最初に初期化ベクトル（IV）を暗

号化し，それと 1 番目の平文ブロックとの XOR 演算によって 1 番目の暗号ブロックを生成する。続いて暗号化された IV をさらに暗号化し，それと 2 番目の平文ブロックとの XOR 演算によって 2 番目の暗号ブロックを生成する。以降もこれを繰り返す。OFB で 513 ビット目から始まる 1 ブロック分のデータ（640 ビットまで）を復号するためには，IV を入力値として各ブロックの暗号化処理を繰り返し，513～640 ビット目の XOR 演算で用いた鍵ストリームを求める必要がある。1 ブロックは 128 ビットであるから，必要な処理回数は，640 ÷ 128 ＝ **5 回**である。

(4)

n：j，l の解説で述べたように，**CBC モード**では，あるブロックの暗号化処理結果が次のブロックの入力値となるため，暗号化時に複数ブロックを並列処理することはできない。一方，復号時には一つ前の暗号ブロックを入力値として XOR 演算をすればよいため，並列処理が可能である。

o：**OFB モード**では，最初に IV と鍵を用いて暗号化処理を行い，鍵ストリームを生成する。次のブロックでは，その鍵ストリームを入力値として，前回と同じ鍵を用いて暗号化処理を行い，当該ブロックで使用する鍵ストリームを生成する。以降も各ブロックでこれを繰り返す。そのため，IV と鍵を用いれば，各ブロックで使用する鍵ストリームを事前に計算することが可能である。

■設問 4

〔試験センターによる解答例〕

(1)鍵は，サーバごとに生成し，Q サービス内で管理される。(26 字)

(2)鍵が危殆化しても，当該鍵が利用されるフォルダ以外には影響がない。(32 字)

(3)・ファイルの名称（7 字）

・おおよそのファイルサイズ（12 字）

(4)p：9

q：62

r：2

s：31

t：8.9

※r と s は順不同

(1) Q サービスの暗号化機能の仕様を表 1 の「暗号化」で確認すると，「**暗号鍵は，サーバごとに生成し，Q サービス内で管理する**」とある。この仕様では，Q サービスに対するクラッキングや，X 社関係者の不正行為によって暗号鍵が悪用され，ファイルが復号されてしまう可能性がある。

(2)一つの鍵を全ての機密フォルダで共有して利用する方法では，その鍵が漏洩する等，何らかの理由によって危殆化した場合には，全ての機密フォルダ内のファイルが復号されてしまう可能性がある。これに対し，下線⑤の方法では，作成されたフォルダごとに鍵を生成し，その鍵は当該フォルダ内に登録されるファイルの暗号化と復号だけに利用される。そのため，あるフォルダの鍵が漏洩する等，**何らかの理由によって危殆化したとしても，当該鍵が利用されるフォルダ以外には影響がない**。

(3)図 7 中には解答に結び付くような記述はないが，表 3 の「ファイル・フォルダ暗号化方式」の説明にある「鍵情報を知らなくても，格納されたファイルやフォルダの名称及び他の属性情報を取得できる場合がある」という記述が参考になる。通常，ファイルを暗号化しても，**ファイル名**までは秘匿されない。ファイルの属性情報として，更新日付，ファイルサイズ等があるが，通常，更新日付は暗号化した際に変更されて元の情報が秘匿化されるのに対し，ファイルサイズはそれほど大きく変化しない。そのため，暗号化しても**おおよそのファイルサイズ**を知ることは可能である。

(4)まず［ q ］から［ t ］について解説し，最後に［ p ］について解説する。

q：英大文字，英小文字，数字の合計なので，**62** である。

r，s：

対数においては，$62^x > 10^{16}$の式に任意の底（ここではlog_{62}を与えた式が成り立つため，次のように変換できる。

$$62^x > 10^{16}$$

$$log_{62}62^x > log_{62}10^{16}$$

対数$log_x a^b$は，blog_xa に変換できる。また$log_{62}62 = 1$ であるため，左辺を次のように変換する。

$x log_{62}62 > log_{62}10^{16}$

$x > log_{62}10^{16}$

続いて対数$log_{62}10^{16}$に任意の底（ここでは“log_{10}”）を与えて式を次のように変換する。

$$x > \frac{log_{10}10^{16}}{log_{10}62}$$

対数$log_x ab$は，$log_x a + log_x b$に変換できる。また，前述のように対数$log_x a^b$は，$b log_x a$に変換できるため，上記の式を図 9 で参考として示された値で計算できるように，次のように変換する。

$$x > \frac{16 log_{10}10}{log_{10}2 + log_{10}31}$$

したがって［ r ］，［ s ］に入るのは，**2**，**31**（順不同）である。

t：$log_{10}10 = 1$であり，分母は図 9 で示された値から次のように算出する。

$$x > \frac{16}{0.301 + 1.491} \fallingdotseq \frac{16}{1.792} = 8.9$$（小数第 2 位を四捨五入）

したがって［ t ］に入るのは **8.9** である。

p：［ t ］に入るのが 8.9 であるから，求めるパスワードの文字数 x（整数）は **9** である。

■設問 5

〔試験センターによる解答例〕

(1)暗号化フォルダに登録されたファイルは，復号した後で，マルウェアスキャンを行うようにする。（44 字）

(2)場合：利用者が，暗号化していないファイルを Web ブラウザで登録した場合（32 字）

修正内容：暗号化されていないバックアップのファイルを自動で削除する。（29 字）

(1)図 7 の項番 3 を見ると，「同期用 FS は，暗号化されたファイルを取得してマルウェアスキャンを行い，……」とあるが，暗号化されたファイルに対してマルウェアスキャンを行っても有効な結果を得ることはできない。有効な結果を得るには，**暗号化フォルダに登録されたファイルは，復号した後でマルウェアスキャンを実施する**必要がある。

(2)平文のファイルを Q サービスに保管するケースとしては，図 7 の項番 3「Web インタフェースを用いて暗号化フォルダにアクセスしたときの処理」にある，利用者が「暗号化フォルダに平文のファイルが登録された場合又は平文のファイルで既存のファイルが更新された場合」がある。図 7 によれば，このとき，同期用 FS は当該ファイルを暗号化して更新する仕様となっている。ところが，その一方で，表 1 の「ファイル管理」【補足説明】項番 1 に「ファイルが更新又は削除された場合，元のファイルはバックアップとして保管される」とあるように，元の（平文の）ファイルが Q サービスに保管され続けることになる。

この状況を防ぐために同期用 FS の拡張機能に行うべき修正内容としては，上記の機能によって作成された平文の**バックアップファイルを自動で削除すること**である。

■設問 6

〔試験センターによる解答例〕

委託先のデータ管理の実態を監査によって把握して監督する。(28 字)

図 5 の「J 社からの要求（概要）」に，「J 社から受託した業務の一部を再委託する場合は，当該委託先に対して本要求と同等の措置を求め，かつ，その実施について監督する」とあるが，この要求への対応が不十分であったと考えられる。問題文の「組織における内部不正防止ガイドライン」に限らず，通常重要なデータを取り扱う業務の委託においては，当該委託先に対し，対象となる業務やデータ管理の実態を監査によって把握して監督することが求められる。

なお，「組織における内部不正防止ガイドライン」には，「4-4.技術・運用管理」の「(16)業務委託時の確認（第三者が提供するサービス利用時を含む）」に，次のような記述がある。

「委託する業務内容と重要情報の重要度に応じて，セキュリティ対策を事前に確認・合意してから契約し，委託先が契約通りに情報セキュリティ対策を実施しているか定期的及び不定期に確認しなければならない」