

平成 27 年度 秋期  
**情報セキュリティスペシャリスト試験**  
**午後 II 問題**

試験時間 14:30 ~ 16:30 (2 時間)

**注意事項**

1. 試験開始及び終了は、監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで、問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は、試験開始の合図があってから始めてください。
4. 問題は、次の表に従って解答してください。

問題番号	問 1, 問 2
選択方法	1 問選択

5. 答案用紙の記入に当たっては、次の指示に従ってください。
  - (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
  - (2) 受験番号欄に受験番号を、生年月日欄に受験票の生年月日を記入してください。  
 正しく記入されていない場合は、採点されないことがあります。生年月日欄については、受験票の生年月日を訂正した場合でも、訂正前の生年月日を記入してください。
  - (3) 選択した問題については、次の例に従って、**選択欄の問題番号を○印で囲んで**ください。○印がない場合は、採点されません。2 問とも○印で囲んだ場合は、はじめの 1 問について採点します。
  - (4) 解答は、問題番号ごとに指定された枠内に記入してください。
  - (5) 解答は、丁寧な字ではっきりと書いてください。読みにくい場合は、減点の対象になります。

[問 2 を選択した場合の例]

選択欄	
1 問 選 択	問 1
	○問 2

注意事項は問題冊子の裏表紙に続きます。  
 こちら側から裏返して、必ず読んでください。

問1 シンクライアント技術を利用したマルウェア対策に関する次の記述を読んで、設問1～5に答えよ。

A社は、従業員数20,000名の金融機関である。A社では、これまで、本店、国内支店及び海外支店で働く従業員間の情報共有、電子メール（以下、メールという）の送受信及びインターネット上のWebサイトアクセスのための環境を整備してきた。現在のPC、サーバ及びネットワーク（以下、OAシステムという）の構成を図1に示す。

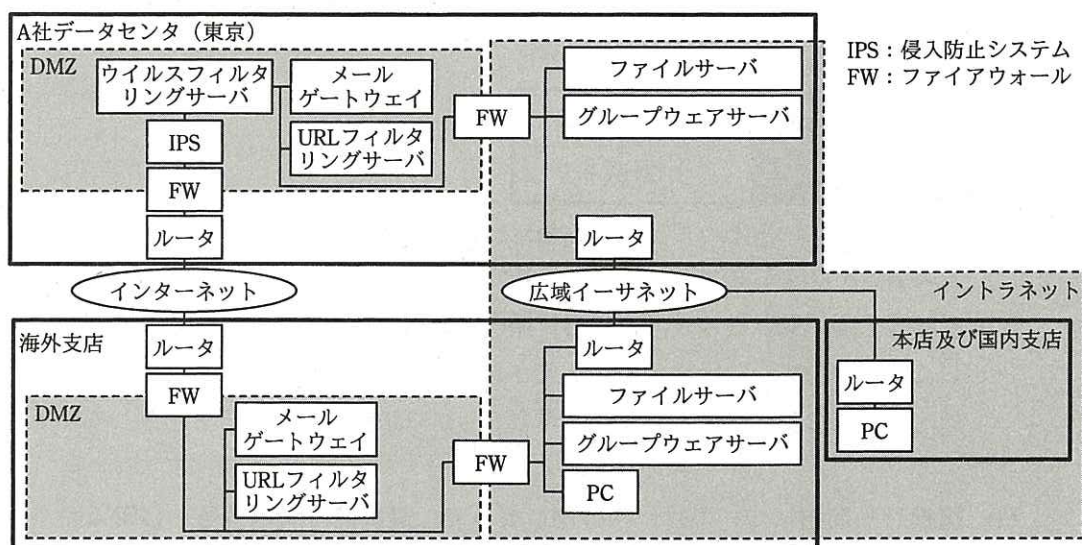


図1 現在のOAシステムの構成

PCには、クライアントアプリケーションソフトウェア（以下、クライアントアプリケーションという）としてWebブラウザ、グループウェアクライアント、オフィスソフトウェア及びPDFリーダーが導入されている。グループウェアサーバは、メールサーバの機能ももっている。利用者は、グループウェアクライアントを利用して情報共有及びメールの送受信を行うことができる。ウイルスフィルタリングサーバは、HTTP通信及びSMTP通信においてファイルのウイルススキャンを行い、ウイルスが検出された場合は、直ちに当該通信を遮断し、ファイルを送受信した従業員と情報システム部の管理者に警告メッセージを送信する。URLフィルタリングサーバは、業務上必要がないWebサイトへのアクセスを禁止する。

A 社は、情報システムのセキュリティ管理の強化及びコストの削減のために、本店及び全支店の PC をシンクライアント（以下、TC という）端末に段階的に移行し、A 社データセンタ（東京）内にサーバを集約することにした。

[マルウェア対策の要件]

TC 端末への移行及びサーバの集約に当たり、情報セキュリティ管理部は、情報システム部に対して、近年重大な脅威となっているマルウェア感染による情報漏えいについて対策を求めた。情報セキュリティ管理部が想定した、マルウェアによる情報漏えいのシナリオは次のとおりである。

(1) 計画立案段階

- ・攻撃者が、A 社従業員のメールアドレス、職場関連の情報を収集する。

(2) 攻撃準備段階

- ・攻撃者が、収集した情報を差出人やメール件名に使用して、従業員がだまされやすい文面のメールを作成する。
- ・攻撃者が、C&C（Command and Control）サーバを準備する。

(3) 初期潜入段階

- ・攻撃者が、メールを従業員に送信する。
- ・メールの添付ファイル又は本文中の URL を従業員に開かせることによって、マルウェアを実行させる。

(4) 基盤構築段階

- ・マルウェアが、C&C サーバの IP アドレスを用いて、C&C サーバとの通信を開始する。

(5) 目的遂行段階

- ・マルウェアが、ファイルサーバ又はグループウェアサーバから機密情報を含んだファイル（以下、機密ファイルという）を盗み出す。
- ・マルウェアが、盗み出した機密ファイルを C&C サーバから指示されたインターネット上のサーバに送信する。

情報セキュリティ管理部は、マルウェアによってファイルサーバとグループウェア

サーバ上の機密ファイルが、インターネット上のサーバに送信されることを防ぐために、情報漏えいのシナリオを踏まえた次の対策を新しい OA システムの要件とした。

(1) マルウェア感染対策（初期潜入段階に対する対策）

要件 1. PC 及び各サーバにおいてウイルス対策ソフトを利用する。

要件 2. ウイルスフィルタリングサーバによって、受信メールの添付ファイル及び Web サイトからダウンロードしたファイルに対するウイルススキャンを行う。

(2) マルウェア感染後の情報漏えい対策（基盤構築段階及び目的遂行段階に対する対策）

要件 3. 認証プロキシサーバを新設し、利用者 ID とパスワードによる利用者認証及びアクセスログの取得を行う。インターネット上の Web サイトへのアクセスは、必ず認証プロキシサーバを経由させる。

要件 4. 基盤構築段階及び目的遂行段階で利用される通信を禁止する。

情報システム部の Z 部長は、部下の Y さんに、要件 1～4 を考慮した OA システムの設計を行い、情報セキュリティ管理部のレビューを受けるよう指示した。

〔新しい OA システムの設計〕

Y さんは、新しい OA システムの設計案（以下、設計案 1 という）を作成した。設計案 1 の構成を図 2 に、設計案 1 における通信を表 1 に、それぞれ示す。

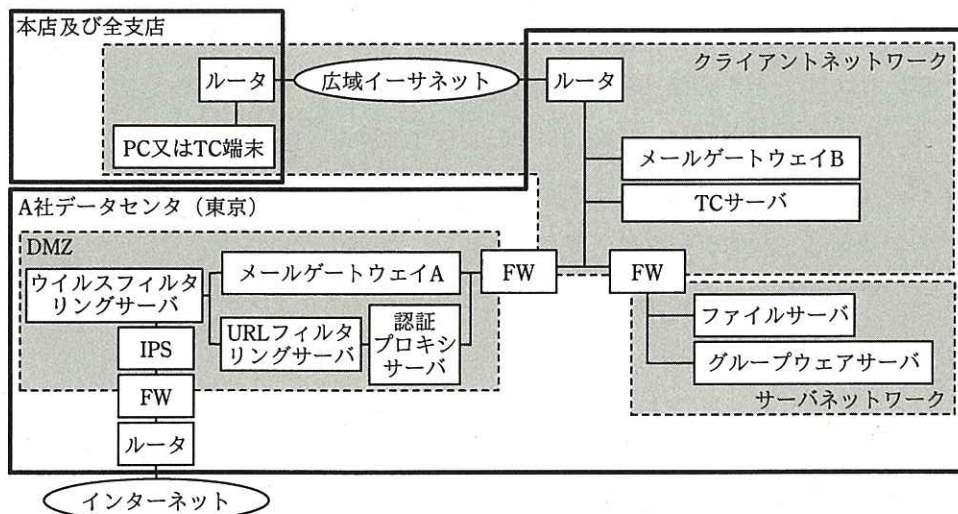


図2 設計案1の構成

表1 設計案1における通信

項番	送信元	宛先	プロトコル
1	PC又はTC端末	TCサーバ	TCサーバ製品の独自プロトコル
2	TCサーバ	ファイルサーバ	Windows ファイル共有プロトコル
3	TCサーバ	グループウェアサーバ	グループウェア独自プロトコル
4	グループウェアサーバ	メールゲートウェイB	SMTP
5	メールゲートウェイB	メールゲートウェイA	SMTP
6	メールゲートウェイA	インターネット上のメールサーバ	SMTP
7	インターネット上のメールサーバ	メールゲートウェイA	SMTP
8	メールゲートウェイA	メールゲートウェイB	SMTP
9	メールゲートウェイB	グループウェアサーバ	SMTP
10	TCサーバ	認証プロキシサーバ	HTTP及びHTTP over TLS (以下、HTTPSという)
11	認証プロキシサーバ	インターネット上のWebサーバ	HTTP及びHTTPS

注記1 DNS及びWindowsのディレクトリサービスの通信は、省略している。

注記2 表及び注記1に記載のない通信はFWによって禁止されている。

注記3 FW、ルータなどTCPコネクションを終端しない機器は送信元及び宛先として記載していない。

設計案1の概要は、次のとおりである。

- ・ネットワークを複数のネットワークに分け、FWでネットワーク間の通信を制限する。
- ・TCには、OS及びクライアントアプリケーションを複数の利用者で共有する、画面転送型又はサーバベース方式と呼ばれる方式を採用する。

- ・ TC サーバの OS 上で、クライアントアプリケーションが稼働する。
- ・ PC にはビューア（TC 端末の機能を提供するソフトウェア）を導入するが、その後、本店及び支店ごとに段階的に PC から TC 端末へ移行する。
- ・ TC 端末及びビューアから TC サーバまでの間は、TC サーバ製品独自のプロトコルで通信し、次のデータを送受信する。
  - デスクトップ及び TC サーバ上で動作するクライアントアプリケーションの画面
  - キーボード、マウスの操作情報
- ・ 認証プロキシサーバは、利用者 ID とパスワードによる利用者認証を行う。次のいずれかの利用者認証の方式を選択できるが、方式 2 を選択する。
  - 方式 1. 利用者が Web ブラウザを起動するたびに認証する。
  - 方式 2. 認証が成功すると、設定された時間が経過するまでは、クライアントの IP アドレスによって認証済みの利用者のみとする。

新しい OA システムは、次のように動作する。

- ・ TC 端末又はビューアを起動して TC サーバにログオンすると、TC サーバが提供するデスクトップが表示される。デスクトップには、各クライアントアプリケーションを起動するためのアイコンがある。
- ・ アイコンをクリックすると、クライアントアプリケーションが TC サーバの OS 上の一つのプロセスとして起動する。TC サーバには、仮想 IP アドレスプール（クライアントアプリケーションのプロセスが利用する仮想 IP アドレスの範囲）が定義されている。クライアントアプリケーションのプロセスは、仮想 IP アドレスプールの中から他のプロセスで利用されていない仮想 IP アドレスを一つ選択して利用する。クライアントアプリケーションのプロセスが終了すると、当該プロセスで利用されていた仮想 IP アドレスは解放され、他のプロセスが起動したときに再利用される。
- ・ グループウェアクライアントの画面で受信メールの添付ファイルのアイコンをクリックすると、当該ファイルが開かれる。このとき、グループウェアクライアントは、グループウェアクライアントの実行環境である TC サーバの作業フォルダに、グループウェアサーバから添付ファイルをダウンロードし、OS の設定でファイル

タイプに関連付けられたクライアントアプリケーションを起動する。

- ・ Web ブラウザ上でクリックしたリンクが、OS の設定でファイルタイプごとに関連付けられたインターネット上のファイルへのリンクであった場合、Web ブラウザは、インターネット上の Web サーバから Web ブラウザの実行環境である TC サーバ上の作業フォルダに当該ファイルをダウンロードし、該当するクライアントアプリケーションを起動する。
- ・ 各従業員には、TC サーバの設定によって、ファイルサーバのフォルダが一つずつ割り当てられている。クライアントアプリケーションの画面からファイル保存の操作を行うと、保存先を選択する画面に D ドライブとしてそのフォルダが表示される。D ドライブを保存先に選択すると、当該ファイルが、クライアントアプリケーションが稼働している TC サーバからファイルサーバに転送される。

#### [マルウェア対策を考慮した修正]

Y さんが設計案 1 について情報セキュリティ管理部のレビューを受けたところ、次の 3 点が指摘された。

指摘 1. 要件 2 のウイルススキャンが行われない場合がある。要件 2 を満たすように対策を強化する必要がある。

指摘 2. 要件 3 の認証プロキシサーバの方式選択について、方式 2 では要件 3 を満たせない。方式 1 を選択すべきである。

指摘 3. FW 及び IPS による通信の制限だけでは要件 4 を満たしていない。対策を追加する必要がある。

Y さんは、情報セキュリティ管理部の指摘を反映した修正案（以下、設計案 2 という）を作成し、情報セキュリティ管理部と Z 部長の承認を得た。設計案 2 では、TC サーバを、用途によってオフィス環境用 TC サーバ（以下、OA 用 TC サーバという）とインターネットアクセス用 TC サーバ（以下、IA 用 TC サーバという）に分けている。また、本店及び全支店でメールによるファイル送信及びインターネット上の Web サイトへのファイルアップロードを、情報漏えい防止サーバ（以下、DLP サーバという）を使って制限する対策を追加している。DLP サーバの仕組みは次のとおりである。

- ・ HTTP 通信及び SMTP 通信でインターネットに送信されるファイルに、住所、氏名、電話番号又は機密、個人情報などの区分を示す文字列が含まれていないかを検査する。
- ・ 機密や個人情報に該当すると判断した場合は、通信を遮断し、ファイル送信を行った従業員と情報システム部の管理者に警告メッセージを送る。

設計案 2 の構成を図 3 に、設計案 2 における通信を表 2 に、それぞれ示す。

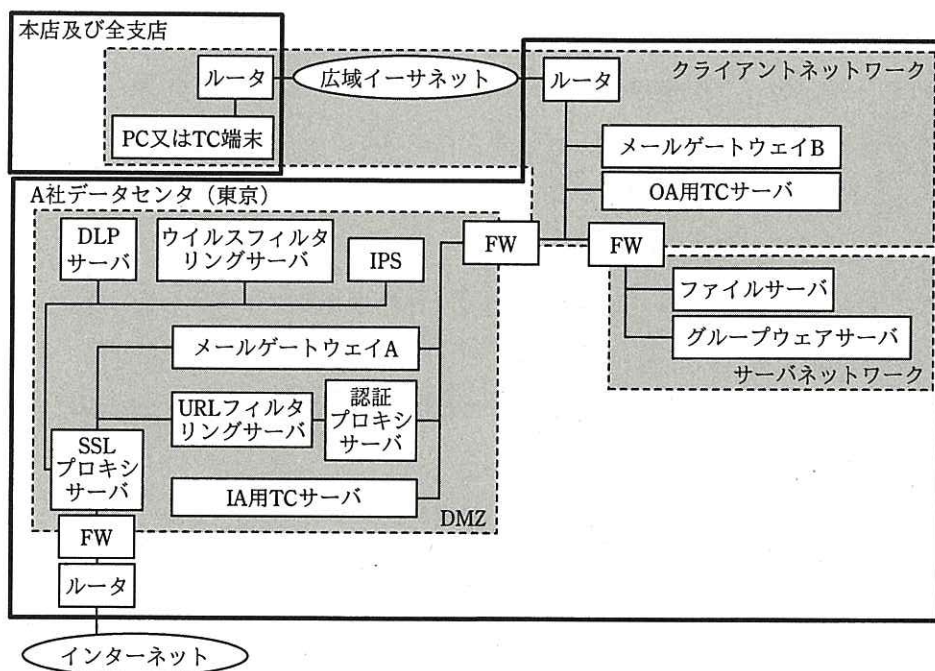


図 3 設計案 2 の構成



表 2 設計案 2 における通信

項番	送信元	宛先	プロトコル
1	PC 又は TC 端末	OA 用 TC サーバ	TC サーバ製品の独自プロトコル
2	OA 用 TC サーバ	ファイルサーバ	Windows ファイル共有プロトコル
3	OA 用 TC サーバ	グループウェアサーバ	グループウェア独自プロトコル
4	グループウェアサーバ	メールゲートウェイ B	SMTP
5	メールゲートウェイ B	メールゲートウェイ A	SMTP
6	メールゲートウェイ A	インターネット上のメールサーバ	SMTP
7	インターネット上のメールサーバ	メールゲートウェイ A	SMTP
8	メールゲートウェイ A	メールゲートウェイ B	SMTP
9	メールゲートウェイ B	グループウェアサーバ	SMTP
10	PC 又は TC 端末	IA 用 TC サーバ	TC サーバ製品の独自プロトコル
11	IA 用 TC サーバ	認証プロキシサーバ	HTTP 及び HTTPS
12	認証プロキシサーバ	SSL プロキシサーバ	HTTP 及び HTTPS
13	SSL プロキシサーバ	インターネット上の Web サーバ	HTTP 及び HTTPS

注記 1 DNS 及び Windows のディレクトリサービスの通信は省略している。

注記 2 表及び注記 1 に記載のない通信は FW によって禁止されている。

注記 3 FW, ルータなど TCP コネクションを終端しない機器は送信元及び宛先として記載していない。

設計案 2 において、利用者が受信メール中の URL をクリックした場合、OA 用 TC サーバ上で Web ブラウザが起動されるが、当該 URL へのアクセスは失敗する。OA 用 TC サーバ及び IA 用 TC サーバの作業フォルダ中のファイルは、定期的に削除される。SSL プロキシサーバは、HTTPS 通信の復号及び再暗号化に用いられる。

[業務要件を踏まえた再修正]

A 社は、一部の国内支店において新しい OA システムの試行運用を開始した。試行運用は成功し、A 社は新しい OA システムを本店及び全支店に展開することを決めた。展開に先立ち、情報システム部が本店及び全支店に新しい OA システムについて説明したところ、海外支店 X から、他の金融機関との共同融資業務及び幹事業務のために、PC 及び支店固有のインターネット接続回線を継続利用したいという要望が上がった。その業務とは、オンラインストレージとメールを使って、複数の金融機関との間で、融資案件の情報を共有し、参加する金融機関の募集を行うというものである。業務の具体的な内容は次のとおりである。

(1) 共同融資業務

- a. 融資案件の幹事の金融機関から、融資案件に対する融資依頼のメールが送られ

てくる。オンラインストレージ上には当該融資案件に関するファイル（以下、案件ファイルという）が置かれており、メールにそれら案件ファイルのリストを含むページの URL が含まれている。

- b. 融資依頼のメール中の URL をクリックしてリストにアクセスする。
- c. リストから案件ファイルを選択し、ファイルサーバにダウンロードする。
- d. 融資案件に融資する場合、幹事の金融機関に対して、返信メールで、参加表明と融資額を連絡する。

## (2) 幹事業務

- e. オフィスソフトウェアを使って案件ファイルを作成し、ファイルサーバに保存する。
- f. ファイルサーバからオンラインストレージに案件ファイルをアップロードする。
- g. 他の金融機関宛ての融資依頼のメールを作成し、オンラインストレージ上の案件ファイルのリストを含むページの URL を、Web ブラウザの画面からメール中にコピーして貼り付ける。
- h. 融資依頼のメールを送信する。

1 融資案件当たりの案件ファイルの合計サイズは、最大 500 M バイトである。海外支店 X では、業務の最繁時間帯の 9:00~10:00 の間、100 名の従業員が、1 名当たり最大 3 件の共同融資業務を行っており、この業務スピードを維持する必要がある。融資案件への融資会社募集は、必要な資金が集まった時点で打ち切られ、幹事の金融機関によって融資先及び融資元との間の契約手続が開始されることから、利益率、リスクが好条件の案件ほど参加表明と融資額を早く連絡する必要がある。幹事業務は、9:00~10:00 の間には行われない。

Y さんは、マルウェア対策に加えて海外支店 X において他の金融機関との共同融資業務及び幹事業務を可能にする修正案（以下、設計案 3 という）を作成した。設計案 3 では、海外支店 X 専用として、ファイルサーバ及び TC サーバが追加されている。

設計案 3 の構成を図 4 に、設計案 3 における通信を表 3 に、それぞれ示す。

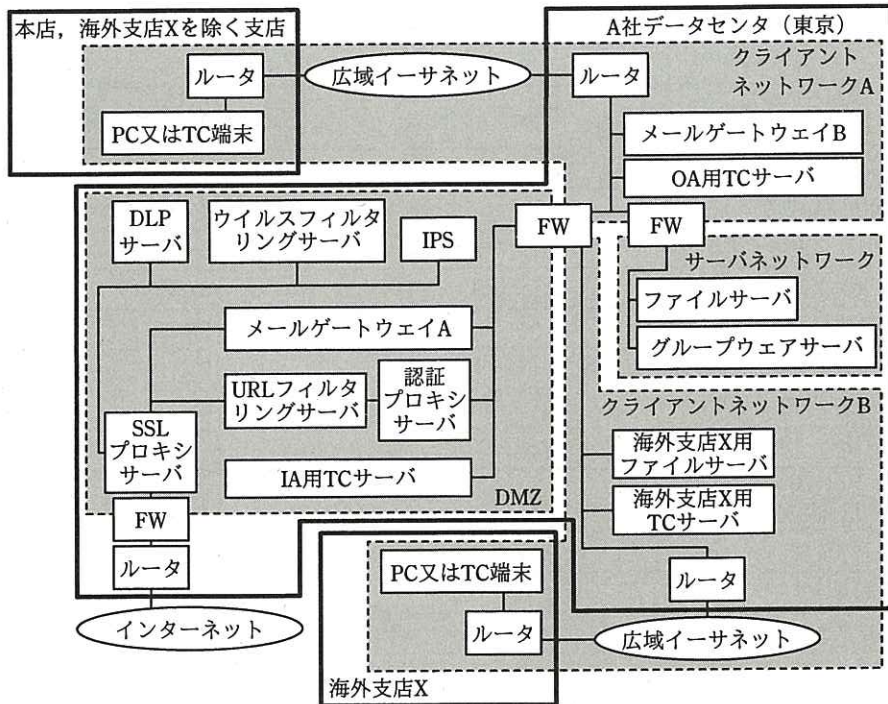


図4 設計案3の構成

表3 設計案3における通信

項番	送信元	宛先	プロトコル
1	PC又はTC端末 (本店, 海外支店Xを除く支店)	OA用TCサーバ	TCサーバ製品の独自プロトコル
2	OA用TCサーバ	ファイルサーバ	Windows ファイル共有プロトコル
3	OA用TCサーバ	グループウェアサーバ	グループウェア独自プロトコル
4	グループウェアサーバ	メールゲートウェイB	SMTP
5	メールゲートウェイB	メールゲートウェイA	SMTP
6	メールゲートウェイA	インターネット上のメールサーバ	SMTP
7	インターネット上のメールサーバ	メールゲートウェイA	SMTP
8	メールゲートウェイA	メールゲートウェイB	SMTP
9	メールゲートウェイB	グループウェアサーバ	SMTP
10	PC又はTC端末 (本店, 海外支店Xを除く支店)	IA用TCサーバ	TCサーバ製品の独自プロトコル
11	IA用TCサーバ	認証プロキシサーバ	HTTP及びHTTPS
12	認証プロキシサーバ	SSLプロキシサーバ	HTTP及びHTTPS
13	SSLプロキシサーバ	インターネット上のWebサーバ	HTTP及びHTTPS
14	PC又はTC端末(海外支店X)	海外支店X用TCサーバ	TCサーバ製品の独自プロトコル
15	海外支店X用TCサーバ	海外支店X用ファイルサーバ	Windows ファイル共有プロトコル
16	海外支店X用TCサーバ	グループウェアサーバ	グループウェア独自プロトコル
17	海外支店X用TCサーバ	認証プロキシサーバ	HTTP及びHTTPS

注記1 DNS及びWindowsのディレクトリサービスの通信は省略している。

注記2 表及び注記1に記載のない通信はFWによって禁止されている。

注記3 FW, ルータなどTCPコネクションを終端しない機器は送信元及び宛先として記載していない。

#### [パフォーマンス検証]

Yさんは、設計案3について、情報セキュリティ管理部とZ部長の承認を得た後、海外支店Xに対して説明会を開いた。海外支店Xは、設計案3が共同融資業務での業務スピード維持に必要なパフォーマンス要件を満たせるのかどうかについて検証を求めた。

Yさんが試算したところ、パフォーマンス要件を満たすには、インターネット接続回線の帯域幅を確保するために大きなコストが必要になることが判明した。Yさんは、海外支店Xについては例外的に、TC端末に移行せずに、システム運用とセキュリティ管理も含めてPC及び支店固有のインターネット接続回線を図1の現状のまま継続利用せざるを得ないと結論付けた。Yさんは、設計案3を更に修正した設計案(以下、設計案4という)を作成し、その内容と修正理由を情報セキュリティ管理部とZ部長に説明した。設計案4の構成を図5に示す。

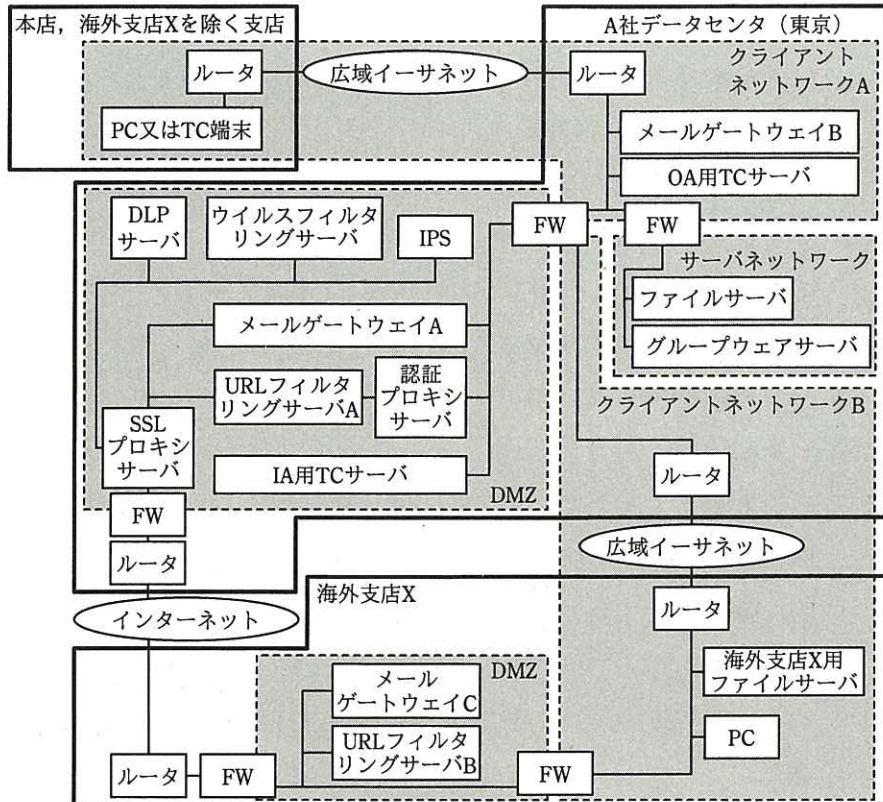


図5 設計案4の構成

情報セキュリティ管理部とZ部長は、海外支店Xのインターネット接続におけるセキュリティ対策について、次の二つを条件として、設計案4を承認した。

- ・①他の支店と同等の技術的対策を行うこと
- ・新しいOAシステムは、国内、海外ともに情報システム部が構築、運用及びセキュリティ管理を行い、情報セキュリティ管理部がセキュリティ管理状況を定期的に監査すること

A社は、条件を満たすように見直した設計案4に基づき、新しいOAシステムの本格運用を開始した。

設問1 [新しいOAシステムの設計]について、(1)、(2)に答えよ。

- (1) 設計案1について、次の(a)～(c)の場面で利用される全ての通信を、それぞれ表1中の項番で答えよ。
  - (a) 本店のTC端末を利用して、グループウェアサーバ上のファイルをファイルサーバに転送する。
  - (b) インターネットからA社にメールが届き、そのメールを国内支店のTC端末を利用して閲覧する。
  - (c) 海外支店のPCを利用して、インターネット上のWebサイトにアクセスする。
- (2) 設計案1において、受信メールの添付ファイルを海外支店のTC端末から開いてマルウェアに感染した場合、マルウェアはどの構成要素上で動作するか。図2中の用語で答えよ。また、その後、マルウェアがファイルサーバ上のファイル及びグループウェアサーバ上のファイルを盗み出してインターネット上のWebサーバに送信するのに利用する全ての通信を、表1中の項番で答えよ。

設問2 [マルウェア対策を考慮した修正]について、(1)～(5)に答えよ。

- (1) 指摘1について、ウイルススキャンが行われないのはどのような場合か。二つ挙げ、それぞれ25字以内で述べよ。
- (2) 指摘2について、方式2が要件を満たせない理由を、技術的要因を含めて75字以内で述べよ。
- (3) 設計案2において、利用者がインターネット上のWebサイトのファイルを閲覧してマルウェア感染が起きた場合、マルウェアはどの構成要素上で動作するか。図3中の用語で答えよ。
- (4) 設計案2において、利用者が受信メールの添付ファイルを開いてマルウェア感染が起きた場合、マルウェアはどの構成要素上で動作するか。図3中の用語で答えよ。
- (5) 設計案2におけるマルウェア対策について、目的遂行段階でマルウェアが利用する二つの通信のうち、FWによって禁止されているのはどの通信か。マルウェアの実行がインターネット上のWebサイトのファイルを閲覧して起きた場合、及び受信メールの添付ファイルを開いて起きた場合のそれぞれにつ

いて、送信元、宛先及びプロトコルを答えよ。

設問3 [業務要件を踏まえた再修正] について、(1), (2)に答えよ。

- (1) 海外支店 X の共同融資業務及び幹事業務のうち、設計案 2 では実現できない項目を全て挙げ、本文中の a~h の記号で答えよ。
- (2) 設計案 3 において、海外支店 X の PC からインターネット上の Web サイトのファイルを開いてマルウェアに感染した場合、及び受信メールの添付ファイルを開いてマルウェアに感染した場合、それぞれマルウェアはどの構成要素上で動作するか。図 4 中の用語で答えよ。

設問4 [パフォーマンス検証] について、(1), (2)に答えよ。

- (1) パフォーマンス要件を満たすために必要な回線速度は何 M ビット/秒か。小数第 1 位を四捨五入して整数で答えよ。ここで、回線使用率は 70%とする。また、1M バイト=10<sup>6</sup>バイト、1M ビット/秒=10<sup>6</sup>ビット/秒とし、制御データ及びエラーによる再送については、回線使用率の前提条件で考慮されているものとする。
- (2) 本文中の下線①を実現するために、図 5 中の海外支店 X の DMZ に追加すべき構成要素を解答群の中から全て選び、記号で答えよ。

解答群

- |                  |               |
|------------------|---------------|
| ア DLP サーバ        | イ IA 用 TC サーバ |
| ウ IPS            | エ OA 用 TC サーバ |
| オ SSL プロキシサーバ    | カ TC サーバ      |
| キ ウイルスフィルタリングサーバ | ク 認証プロキシサーバ   |

設問5 設計案 4 において、監査とセキュリティ管理の役割を一つの組織にもたせた場合、どのような不都合が起こるか。30 字以内で述べよ。

問2 データの取扱いに関する次の記述を読んで、設問1～6に答えよ。

V社は、CM、プロモーションビデオなどのコンテンツを受託制作する従業員数500名の会社である。従業員はコンテンツの素材撮影のために国内外に出張する機会が多い。V社は、コンテンツの制作の一部を他の事業者へ委託している。委託先事業者（以下、委託先という）には個人で事業を行うデザイナーやクリエイターも多い。

コンテンツの受託制作では、必要なデータを顧客から受け取り、その全部又は一部を委託先と共有して作業を進める場合がある。受け取ったデータだけでなく、当該データから派生した中間データ、及び、撮影又は作成された素材も含めて、適切な保護が必要である。

V社では、従業員には、業務に応じてデスクトップPC（以下、DPCという）又はノートPC（以下、NPCという）を貸与している。従業員の識別と認証に必要な利用者情報は、ディレクトリサーバ（以下、Dサーバという）で管理している。DサーバはIT部が運用している。

[オンラインストレージサービスの導入決定]

V社では、業務効率の向上のために、クラウドベースのオンラインストレージの導入を決定し、IT部のM部長を導入責任者に任命した。オンラインストレージの用途は、次のとおりである。

- ・出張者と内勤者の間で、サイズが大きいデータを共有する。
- ・委託先とV社の間で、データを共有する。
- ・デモやその他の目的のためにデータを取引先に送信する。
- ・NPCなどにプレゼンテーション資料を配布する。

M部長は、IT部内のチームに複数のオンラインストレージサービスを比較検討させた結果、X社のQサービスを採用することにした。

[Qサービスの概要]

Qサービスの利用者は、インターネット経由で、Qサービスに任意のファイルを保管できる。Qサービスの概要を表1に、Qサービスの利用者用の専用アプリケーション



ソフトウェア（以下、同期アプリという）の概要を表 2 に、V 社における Q サービスの利用方法を図 1 に、それぞれ示す。

表 1 Q サービスの概要

項目	説明
アカウント管理	<ul style="list-style-type: none"> <li>・利用者に、個別のアカウントを割り当てる。</li> <li>・利用企業は、利用者のアカウントを自社で登録して管理するための機能（以下、管理者機能という）を利用できる。アカウントをもたない者も、Q サービスの一部の機能は利用できる（項目“ファイル管理”参照）。</li> </ul>
管理者機能	<ul style="list-style-type: none"> <li>・管理者は、アカウントの作成・停止・再開・廃止、パスワードの初期発行・再発行、ファイル及びフォルダへのアクセス履歴の閲覧、その他の管理のための機能を利用できる。</li> </ul>
利用者識別・認証	<ul style="list-style-type: none"> <li>・利用者 ID とパスワードを用いて利用者を識別・認証する。</li> <li>・利用者は、インタフェースを利用して、パスワードを変更できる。</li> </ul>
ファイル管理	<ul style="list-style-type: none"> <li>・各アカウントには、それぞれ専用のフォルダ（以下、ルートフォルダという）が与えられる。利用者が登録したファイルやフォルダは、ルートフォルダの下に配置される。</li> <li>・利用者は、インタフェースを利用して、次の機能を実行できる。 <ul style="list-style-type: none"> <li>- ファイルの登録・更新・削除・取得・プロパティの閲覧</li> <li>- フォルダの作成・削除・閲覧・プロパティの閲覧</li> <li>- バックアップからのファイルの復元・取得・削除（補足説明 1 参照）</li> <li>- 他の利用者へのファイル又はフォルダのアクセス権の付与・変更（補足説明 2 参照）</li> <li>- ファイルにアクセスするための共有リンクの作成・削除（補足説明 3 参照）</li> </ul> </li> </ul> <p>【補足説明】</p> <ol style="list-style-type: none"> <li>1. 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。利用者は、バックアップとして保管されたファイルのうち、バックアップから削除が行われていないものを、復元・取得できる。</li> <li>2. 他の利用者に付与できる権限には“読み”と“読み書き”の 2 種類がある。“読み”は、ファイルの取得機能などの、ファイルやフォルダの変更を伴わない機能を利用する権限である。“読み書き”は、“読み”の権限に加え、ファイルの更新機能などの、変更を伴う機能を利用する権限である。</li> <li>3. アカウントをもたない者にファイルを配布するための URL を“共有リンク”という。Web ブラウザで当該 URL にアクセスすると利用者認証なしにファイルを取得できる。</li> <li>4. アカウントが廃止されると、そのアカウントで登録したファイルとフォルダが削除される。</li> </ol>
インタフェース	<ul style="list-style-type: none"> <li>・同期アプリ、Web インタフェース、API の三つのインタフェースがある。 <ul style="list-style-type: none"> <li>- 同期アプリの機能については、表 2 に概要をまとめる。</li> <li>- Web インタフェースを用いる利用者は、Web ブラウザで Q サービスの Web サーバ（w.example.com）にアクセスし、Q サービスの各機能を利用する。</li> <li>- API を用いて、Q サービスと連携するアプリケーションソフトウェアを開発できる。</li> </ul> </li> </ul>
暗号化	<ul style="list-style-type: none"> <li>・同期アプリと Q サービス間の通信、及び Web ブラウザと Q サービスの Web インタフェース間の通信は、TLS で暗号化される。</li> <li>・Q サービスは複数のサーバで構成されており、ファイルは、他の利用企業又は個人利用者のファイルと同じサーバに保管される場合がある。登録されたファイルは、暗号化して保管される。暗号鍵は、サーバごとに生成し、Q サービス内で管理する。利用者が Q サービスのインタフェースを利用してファイルにアクセスすると、Q サービスは、ファイルを復号した後に引き渡す。</li> </ul>

注記 Q サービスでは、“利用者”とは、アカウントをもつ者だけを指す。

表 2 同期アプリの概要

項目	説明
ファイル管理	・表 1 の項目 “ファイル管理” の機能を提供する。
同期機能	<ul style="list-style-type: none"> <li>・同期アプリは、利用者の PC のローカルディスク上に特別なフォルダ（以下、同期用フォルダという）を作成する。</li> <li>・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。例えば、利用者が同期用フォルダ配下に複製されたファイルを更新した場合、更新内容は、Q サービスの該当ファイルにも適用される。また、更新されたファイルについて、他の利用者にはアクセス権が付与されていた場合、他の利用者の PC の同期アプリが Q サービスの該当ファイルを同期用フォルダにコピーする。</li> </ul>
同期管理	<ul style="list-style-type: none"> <li>・同期機能について設定を行う機能を提供する。自動的な同期を行わない場合は、その旨を設定できる。</li> <li>・同期の状況を表示する。</li> </ul>
その他	<ul style="list-style-type: none"> <li>・同期アプリは、Q サービスの A サーバ (a.example.com) と通信し、各処理を行う。プロキシサーバを経由した通信もサポートしている。</li> <li>・同期アプリは、X 社がインターネットで配布しており、誰でもダウンロードできる。</li> </ul>

<ul style="list-style-type: none"> <li>・Q サービスの利用に関する社内の管理は IT 部が主管する。</li> <li>・IT 部は、業務上 Q サービスの利用が必要な V 社の従業員及び委託先の作業員に対してアカウントを作成する。</li> </ul>
---

図 1 Q サービスの利用方法案（抜粋）

### 〔Q サービスの試験導入〕

M 部長は、Q サービスの導入に先だって、3 か月間の試験導入をすることにした。オンラインストレージの利用が想定される部門の中から、試験導入への参加者を偏りなく選ぶことにし、最終的に 30 名の参加者を決定した。この中には、委託先の 5 名のクリエイターが含まれていた。試験導入では、次の項目を確認することにした。

- ・機能は、利用目的に照らし、必要十分で使いやすいか。
- ・管理は、シンプルで、実用に耐えるか。
- ・セキュリティ及びその他の問題点がないか。

以降、Q サービスについては、V 社が利用する部分だけに限定して述べる。

### 〔Q サービスの試験導入において表出した問題〕

試験導入の結果、機能及び管理については大きな問題は発見されなかった。しかし、セキュリティについては、同期アプリが、マルウェア感染を拡散させるという問題が認識された。

実際に発生した事件は次のとおりである。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。そのことに気付かずにクリエイタが Web インタフェースを使って当該ファイルを 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 Q サービスから同期用フォルダにコピーした。本件では、それぞれの PC にインストールされていたウイルス対策ソフトが感染ファイルを検知したので、大事には至らなかった。しかし、V 社では、事態を重く受け止め、対応について検討することになった。

### 〔Q サービス利用方法の見直し〕

M 部長は、PC のウイルス対策ソフトだけではなく、複数の対策が必要だと考え、IT 部の U さんに、情報セキュリティ室の R 主任の支援を受けて、マルウェア感染ファイルの拡散について対応を検討するように指示した。

U さんは、検討を進め、専用のサーバ（以下、同期用 FS という）及び専用のディスク（以下、同期ディスクという）を介して、社内ネットワークに接続された PC と Q サービス間でのファイルの交換を行う仕組みを提案した。そのネットワーク構成を図 2 に、ファイル交換の仕組みの概要を図 3 に、同期用 FS の機能の説明を図 4 に示す。

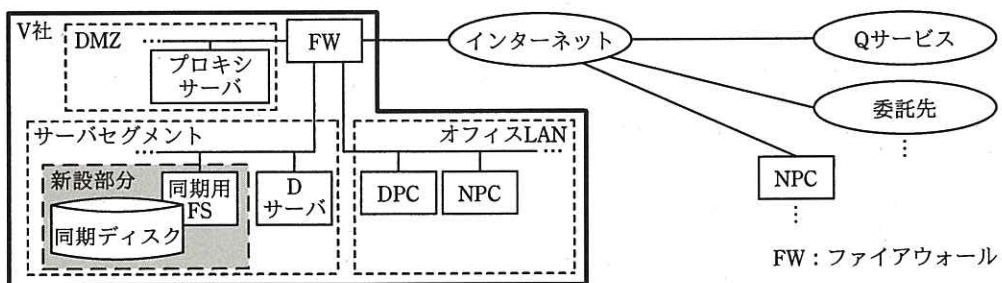


図 2 ネットワーク構成

- ・同期用 FS は、Q サービスに登録された利用者のアカウントのルートフォルダ及びその配下のフォルダ（以下、Q サービス利用者フォルダという）を監視し、新たに登録された又は更新されたファイルがある場合は、それを取得してマルウェアスキャンを行った後、同期ディスクに保管する。
- ・①同期アプリの利用を禁止する。
- ・同期用 FS へのアクセスは、FW によって、オフィス LAN からだけに限定する。

図 3 ファイル交換の仕組みの概要

#### 1. ファイルの同期

・ルートフォルダの複製を同期用 FS 内の同期ディスクに保持し、ファイルを同期する。同期は次のように行う。

A) Q サービス利用者フォルダにおいて、ファイルの登録又は更新があった場合は、当該ファイルを取得してマルウェアスキャンを行う。その結果、問題がなければ同期ディスクに反映する。マルウェアが検知されたら、Q サービス利用者フォルダにある当該ファイルを削除し、もし対応するファイルが同期ディスクに存在する場合はそれも削除する。登録・更新以外の変更があった場合は、同等の変更を同期ディスクに反映する。

B) 同期ディスクのファイルに変更があった場合は、Q サービス利用者フォルダにある対応するファイルに反映する。

#### 2. フォルダの同期

・Q サービス利用者フォルダに変更があった場合は、同期ディスクの対応するフォルダに反映する。

・同期ディスクのフォルダに変更があった場合は、対応する Q サービス利用者フォルダに反映する。

#### 3. アカウントとアクセス制御

・D サーバに登録された従業員の利用者情報と Q サービスのアカウントの対応表をもつ。

・同期ディスクにアクセスがあった場合、D サーバと連携して従業員を識別した後、前記の対応表を基に利用者のアカウントを判別する。この結果に基づいて、次の処理を許可する。

A) 判別されたアカウントの Q サービス利用者フォルダ又はそこにあるファイルに対応する同期ディスクのフォルダ又はファイル：全ての処理

B) 他の利用者のファイル又はフォルダに対応する同期ディスクのファイル又はフォルダ：判別されたアカウントに付与された権限内の処理

#### 4. 補足事項

・Q サービスに保管されたバックアップのファイルについて、同期用 FS は一切処理を行わない。

図 4 同期用 FS の機能の説明（抜粋）

U さんがこれらの検討結果を M 部長に報告したところ、②試験導入において表出した問題を踏まえると、同期用 FS には、マルウェア対策に関して追加すべき機能があると指摘された。 U さんは追加機能を提案し、M 部長は、U さんの提案どおり対応を進めることを承認した。その後、Q サービスと同期用 FS の利用が、全社で開始された。

#### [顧客からの要求]

V 社で Q サービスの利用を開始してから 1 年が経過した頃、重要な顧客である J 社から、情報セキュリティに関して新しい要求の通知があった。J 社の別の委託先において、J 社が開示した新製品に関する CAD データが漏えいするという事件が発生し、対策の一環として、J 社が重要なデータを開示する全ての委託先に対して、新たな要求を課す方針になったとのことであった。J 社からの要求を図 5 に示す。

- J社が開示する全ての重要な情報（以下、J社重要データという）について、次の措置を行うこと
- ・業務上、必要最小限の者しかJ社重要データにアクセスできないように管理する。
  - ・J社重要データをインターネット上に送信する場合には、暗号化する。
  - ・J社重要データを社外に保管する場合には、暗号化する。
  - ・J社重要データを可搬型機器又は可搬型デバイスに保管する場合には、暗号化する。
  - ・業務上不要となったJ社重要データは、直ちに、J社に返却するか、削除する。
  - ・何らかの事故が発生した場合に備え、非常時の連絡体制・手順を確立する。
  - ・J社重要データについて、法令による保護が受けられるように、十分に配慮して管理する。
  - ・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。

図5 J社からの要求（概要）

次は、J社からの要求に関する、M部長とUさんとの会話である。

Uさん：J社から受け取るデータの大半はJ社重要データですが、当社は、J社の要求を満たしていないと思います。

M部長：お客様のデータの保護は最優先事項だ。最近、J社以外にも、複数のお客様から、データの取扱いについての問合せや要求が寄せられている。この機会に、当社の現状を調査し、必要なら見直すことにしよう。

Uさん：分かりました。ところで、法律の規定との関係はどうでしょう。お客様のデータは、で規定されているに該当しますか。

M部長：で規定されているに該当するためには、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、及びこと、の三つの要件を満たす必要がある。秘密として管理されているというためには、その情報が、客観的に見て秘密として管理されている状態になっていなければならない。

Uさん：他の法令はどうでしょうか。

M部長：の235条で規定されている窃盗罪は、他人の財物を窃取した場合に適用される。しかし、情報そのものは物ではなく、財物には当たらないので、適用は難しいという解釈があるようだ。思想又は感情を創作的に表現したと考えられるデータであれば、の保護の対象となる。また、サーバなどの電子計算機に接続して行う不正行為に焦点を当てたがある。ただし、はネットワークを通じて行われる攻撃を対象としているので、攻撃対象の機器を直接操作するケースは

対象外だ。

Uさん：ありがとうございます。教えていただいたことも参考に調査を進めます。

#### 〔顧客データの取扱要件〕

Uさんは、受託業務で顧客から開示を受けた重要なデータ（以下、顧客データという）の取扱状況を調査し、M部長に報告した。M部長は、調査結果を見て、顧客データの取扱いについて改善が必要だと判断した。M部長は、Uさんに、J社の要求を満たすような顧客データの取扱要件及びその実装方法、並びにその他の必要な措置について検討して提案するように指示した。

Uさんは、業務上の必要性のある従業員だけがアクセスできる場所への顧客データの保管、及び顧客データを NPC 又はオンラインストレージに保管する場合の暗号化について検討した。

#### 〔NPC のディスクの暗号化〕

Uさんは、顧客データの暗号化のため、NPC のディスクの暗号化、及びオンラインストレージに登録するデータの自動暗号化の導入を検討した。

Uさんが検討した、NPC のディスクの暗号化方式を表3に示す。

表3 NPC のディスクの暗号化方式

名称	説明
フルディスク暗号化方式	ディスク内の全ての領域を暗号化する方式。PC の全ディスクにこの方式を用いた場合、パスワードがないと <b>g</b> を起動できない。起動後、データの保護は、PC の <b>g</b> が提供する機能に委ねられる。本方式に対応する製品の多くは、PC が休止モードになる際にメモリの内容を書き出すハイバネーション用ファイルの <b>h</b> に対応している。
仮想ディスク暗号化方式	コンテナと呼ぶ仮想的な入れ物を用いて暗号化する方式。コンテナは仮想ディスクとして機能する。コンテナ内にアクセスする場合、利用者の認証が行われる。認証に成功すると、一定の間、通常のディスクと同様に、コンテナにファイルやフォルダを保管したり取り出したりすることができる。データは暗号化された上でコンテナ内に保管される。コンテナは、PC のデータディスク、USB メモリなどに置かれる。スワップ領域やハイバネーション用ファイルには <b>h</b> されていない状態のデータが存在する可能性があるが、これらは保護されない。
ファイル・フォルダ暗号化方式	ファイル単位・フォルダ単位で暗号化する方式。暗号化されたデータは、一つのファイルになる。当該ファイルへのアクセス権があれば、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。

Uさんは、検討した結果、フルディスク暗号化方式を採用することを提案した。

次は、暗号化製品に関する、UさんとR主任との会話である。

Uさん：幾つかの暗号化製品の説明書に“暗号の利用モード”や“CBC モード”という記述がありました。これは何でしょうか。

R主任：利用モードとは、ブロック暗号アルゴリズムを用いてブロック長よりも長いデータを暗号化する際に使われる技術のことだ。CBC モードは、よく使われる利用モードの一つだよ。

Uさん：利用モードは他にもあるのですか。

R主任：図 6 に代表的な暗号の利用モードがまとめられているので見てごらん。ブロック暗号アルゴリズムの利用時には、暗号化の目的や利用方法に合わせて、適切な利用モードを選ぶ必要がある。例えば、③ディスクやファイルの暗号化に ECB モードをそのまま用いるのは、セキュリティ上の問題がある。

利用モードによって、ランダムアクセス時の性能が大きく異なる場合もある。例えば、512 バイトの平文 P を、ブロック長が 128 ビットのブロック暗号アルゴリズムで暗号化した暗号文 C があり、この暗号アルゴリズムでは平文と暗号文の長さは同じとする。平文 P において 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、平文 P の修正に対応して暗号文 C を修正するためには、暗号化処理を、ECB モードでは  回、CBC モードでは  回実行しなければならない。

また、別の暗号文 C' で、513 ビット目から始まる 1 ブロック分のデータを復号するためには、暗号化処理又はその逆処理を、ECB モードでは  回、CBC モードでは  回、OFB モードでは  回実行する必要がある。

複数ブロックの並列処理は、 の場合、暗号化時は不可能だが、復号時は可能だ。 の場合は、鍵ストリームに相当するデータを事前に計算することができる。

ただし、一部の利用モードは、特定の攻撃に弱いので注意が必要だ。

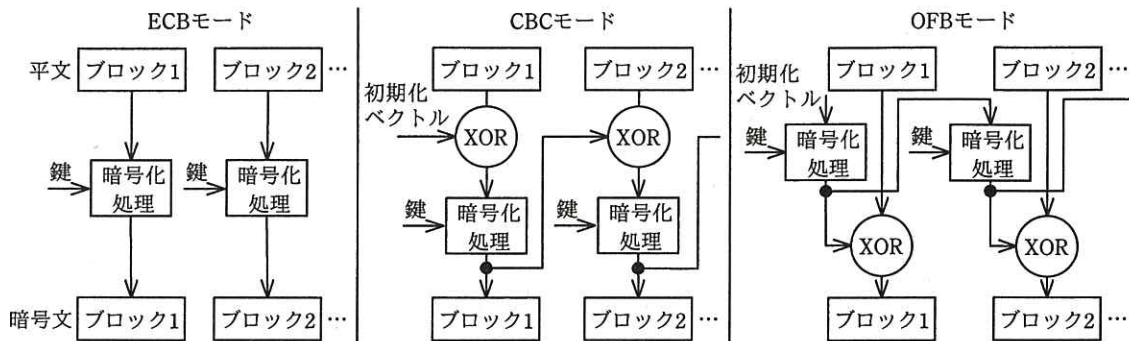


図6 代表的な暗号の利用モード

〔同期用 FS の機能拡張〕

表1に示したように、Qサービスは、元々、登録されたファイルを自動的に暗号化する機能をもつ。しかし、Qサービスの暗号化機能は、④Qサービスに対するクラッキングやX社自身のある種の行為に対して効果が期待できない場合があり、これを補完する措置が必要と考えられた。一方、V社内では、Qサービスの有益性が高く評価されており、継続利用したい。そこで、Uさんは、同期用FSの機能を拡張し、Qサービスに登録する一部のファイルを自動的に暗号化する措置を提案した。同期用FSの拡張機能を図7に、ファイルの暗号化と復号のフローを図8に、それぞれ示す。



1. 機密フォルダと暗号化フォルダの定義・導入
  - ・利用者が同期ディスク中のフォルダに“\_c1”で始まる名称を付けると、そのフォルダは機密フォルダになる。機密フォルダの同期先となるQサービス上のフォルダを暗号化フォルダという。
2. 機密フォルダにアクセスしたときの処理
  - ・利用者が機密フォルダにファイルを登録した場合又は機密フォルダ内のファイルを更新した場合、同期用FSは、ファイルを暗号化した上で、Qサービス上の暗号化フォルダに登録するか、暗号化フォルダ内のファイルを更新する。
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
  - ・利用者は、暗号化フォルダにファイルを登録する場合又は暗号化フォルダ内のファイルを更新する場合、事前に、指定された鍵と暗号化ソフトを用いてファイルを暗号化する（“4. 暗号化のアルゴリズムと鍵”参照）。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、マルウェアが検知されなければ、復号した上で、同期ディスク中の対応する機密フォルダに配置する。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、同期用FSは当該ファイルを暗号化して更新した後、利用者に警告メールを送信する。また、暗号化された当該ファイルは、初めから正しく暗号化されたファイルで更新された場合と同様の手続で、同期ディスクに同期される。
  - ・利用者は、暗号化フォルダからファイルを取得した場合、指定された鍵と暗号化ソフトを用いて復号した上で利用する。
4. 暗号化のアルゴリズムと鍵
  - ・暗号化のアルゴリズムは鍵長 128 ビットの AES、暗号の利用モードは CBC モードとする。
  - ・同期用FSは、機密フォルダ又は暗号化フォルダが作成された際に、作成されたフォルダごとに数字 16 文字のパスワードをランダムに生成し、さらにそれを基に鍵を生成する。⑤生成された鍵は、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。ただし、名称が“\_c1”で始まるサブフォルダがある場合は、そのフォルダを別の機密フォルダ又は暗号化フォルダとみなし、新しいパスワード及び鍵を割り当てる。
  - ・同期用FSは、生成したパスワードを、当該フォルダの利用者に電子メールで通知する。
  - ・暗号化ソフトは、暗号化と復号の機能をもつ PC 用ソフトウェアであり、利用者に配布される。

図 7 同期用 FS の拡張機能（抜粋）

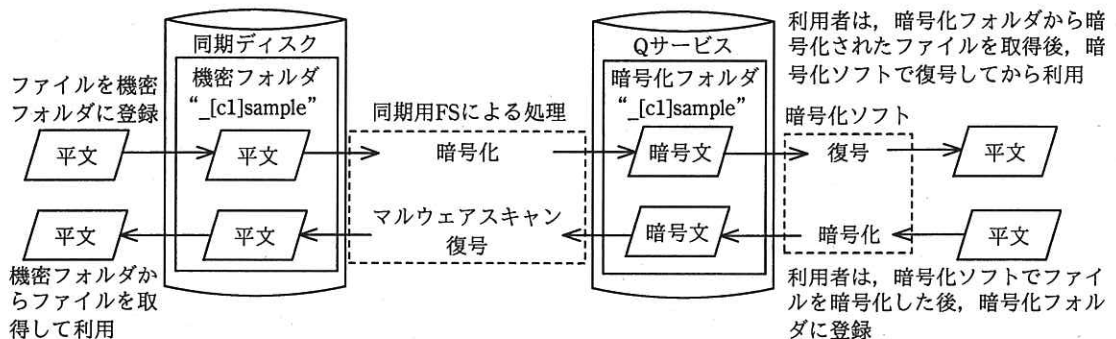


図 8 同期用 FS によるファイルの暗号化と復号のフロー（概要）

Uさんは、図7の方法では、⑥暗号化対象ファイルに関する情報の一部は秘匿されませんが、セキュリティ上容認できると考えた。

Uさんが図7のパスワードについてR主任に相談したところ、R主任は問題を指摘した。R主任は、図9を示し、数字16文字のパスワードの場合の数は、英数字 p 文字のパスワードの場合の数より小さいことを説明した。また、この場

合の数は、最近のコンピュータの能力向上を考慮すると、いつまでも安全とはいえないと指摘した。Uさんは、R主任の指摘を受けて、パスワードの構成を見直した。

英数字  $x$  文字のパスワードについて、その場合の数が、数字 16 文字のパスワードの場合の数より大きくなる最小の  $x$  を考える。ただし、大文字と小文字は区別する。

次の式から、求めるパスワードの文字数  $x$  は  $\boxed{p}$  となる。

$$\boxed{q}^x > 10^{16}$$

$$x > \frac{16 \log_{10} 10}{\log_{10} \boxed{r} + \log_{10} \boxed{s}} = \boxed{t}$$

参考  $\log_{10} 2 \doteq 0.301$ ,  $\log_{10} 3 \doteq 0.477$ ,  $\log_{10} 13 \doteq 1.114$ ,  $\log_{10} 31 \doteq 1.491$

図9 パスワードの検討

[レビューと修正]

Uさんは、IT部と情報セキュリティ室のメンバ（以下、WGという）に、顧客データの取扱要件とその実装方法の案についてのレビューを依頼した。レビューの結果、オンラインストレージについて、次の点が指摘された。

- ・⑦マルウェア感染ファイルの拡散防止対策が不十分である。
- ・⑧暗号化フォルダに登録された一部のファイルが、平文のままQサービスに保管され続ける場合がある。

Uさんは、これらの指摘について検討し、修正案を作成した。修正案について、再度WGでレビューした結果、指摘は解決されていることが確認された。

[M部長の最終確認]

Uさんは、修正案及びその他の必要な措置について、M部長に報告した。

M部長：修正案は技術的に妥当であり、効果がある。当社は委託先との契約の中で、顧客データについて目的外利用の禁止と適切な管理を委託先に要求している。だが、事故の発生を防ぐ点で十分だろうか。

Uさん：当社の現状について調査した結果、委託先の管理が不十分だったので、IPAが公表している“組織における内部不正防止ガイドライン”を参考にして、技術的対策とは別に⑨対策をまとめました。

M 部長は U さんの提案を承認し、提案どおり見直しが行われることになった。

設問 1 [Q サービス利用方法の見直し] について、(1)、(2)に答えよ。

- (1) 図 3 中の下線①について、この措置は、マルウェア感染ファイルの拡散がどのように起こることを想定したものか。40 字以内で具体的に述べよ。
- (2) 本文中の下線②について、同期用 FS にどのような機能を追加すればよいか。追加機能の内容を、30 字以内で具体的に述べよ。

設問 2 [顧客からの要求] について、(1)、(2)に答えよ。

- (1) 本文中の  ,  ~  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 刑法            | イ 個人情報保護法   |
| ウ サイバーセキュリティ基本法 | エ 情報公開法     |
| オ 著作権法          | カ 犯罪収益移転防止法 |
| キ 不正アクセス禁止法     | ク 不正競争防止法   |
| ケ マイナンバー法       | コ 民法        |

- (2) 本文中の  ,  に入れる適切な字句を、 は 5 字以内で、 は 15 字以内でそれぞれ答えよ。

設問 3 [NPC のディスクの暗号化] について、(1)~(4)に答えよ。

- (1) 表 3 中の  ,  に入れる適切な字句をそれぞれ 5 字以内で答えよ。
- (2) 本文中の下線③について、セキュリティ上の問題を、45 字以内で具体的に述べよ。
- (3) 本文中の  ~  に入れる適切な数値を答えよ。
- (4) 本文中の  ,  に入れる適切な暗号の利用モードを、図 6 中の三つの利用モードの中から選んで答えよ。

設問 4 [同期用 FS の機能拡張] について、(1)~(4)に答えよ。

- (1) 本文中の下線④について、Q サービスの暗号化機能の効果が期待できないのは、Q サービスのどのような仕様によるものか。30 字以内で述べよ。
- (2) 図 7 中の下線⑤について、別の方法として、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がある。これらの二つの方法を比較した場合に、  
下線⑤の方法が優れている点は何か。35字以内で具体的に述べよ。

(3) 本文中の下線⑥について、暗号化対象ファイルに関するどのような情報が秘匿されないか。二つ挙げ、それぞれ15字以内で答えよ。

(4) 本文中又は図9中の  ~  に入れる適切な数値を答えよ。  
 ~  は整数で、 は小数第2位を四捨五入して、小数第1位まで求めよ。

設問5 [レビューと修正] について、(1)、(2)に答えよ。

(1) 本文中の下線⑦について、指摘に対応するには、図7の拡張機能をどのように修正すればよいか。修正内容を、50字以内で具体的に述べよ。

(2) 本文中の下線⑧について、どのような場合にファイルが平文のままQサービスに保管され続けるのか。35字以内で具体的に述べよ。また、この状況を防ぐには、同期用FSの拡張機能をどのような修正を行えばよいか。修正内容を30字以内で述べよ。

設問6 本文中の下線⑨について、Uさんがまとめた対策を、35字以内で述べよ。

[ メモ用紙 ]

[ メモ用紙 ]

[ メモ用紙 ]

6. 退室可能時間に途中で退室する場合には、手を挙げて監督員に合図し、答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ~ 16:20
--------	---------------

7. **問題に関する質問にはお答えできません。** 文意どおり解釈してください。
8. 問題冊子の余白などは、適宜利用して構いません。
9. 試験時間中、机の上に置けるものは、次のものに限ります。  
なお、会場での貸出しは行っていません。  
受験票、黒鉛筆及びシャープペンシル (B 又は HB)、鉛筆削り、消しゴム、定規、時計 (時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可)、ハンカチ、ポケットティッシュ、目薬  
これら以外は机の上に置けません。使用もできません。
10. 試験終了後、この問題冊子は持ち帰ることができます。
11. 答案用紙は、いかなる場合でも提出してください。回収時に提出しない場合は、採点されません。
12. 試験時間中にトイレへ行きたくなったり、気分が悪くなったりした場合は、手を挙げて監督員に合図してください。

試験問題に記載されている会社名又は製品名は、それぞれ各社又は各組織の商標又は登録商標です。  
なお、試験問題では、™ 及び ® を明記していません。