全問が必須問題です。必ず解答してください。

問1　インターネットを利用した振込業務の情報セキュリティリスクに関する次の記述を読んで，設問1～5に答えよ。

F社は，従業員数70名の商社であり，主にインテリアやギフト用品の仕入れ，販売を行っている。F社には，総務部，企画管理部，商品部，営業部がある。

F社では，3年前に最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，情報セキュリティポリシ及び情報セキュリティ関連規程を整備した。CISOは社長が兼務しており，情報セキュリティ委員会の事務局は，総務部が担当している。また，各部の部長は，情報セキュリティ委員会の委員，及び自部における情報セキュリティ責任者を務めている。各情報セキュリティ責任者は，自部の情報セキュリティを確保，維持及び改善する役割を担っており，さらに自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。F社の企画管理部には，経営企画課及び経理課がある。経営企画課のS主任は，企画管理部全体の情報セキュリティリーダである。

〔インターネットバンキングサービスの利用〕

F社は，C銀行に口座をもち，C銀行が提供する法人向けインターネットバンキングサービス（以下，IBサービスという）を次の目的で利用している。

・自社の口座の残高及び入出金明細の照会
・取引先への商品代金の振込，運送業者への輸送費の振込，従業員への給与振込など

F社でIBサービスを利用しているのは，経理課のL課長，M主任及びNさんの3名（以下，経理担当者という）である。振込に関する取引先との電子メール（以下，電子メールをメールという）連絡などは各自の会社貸与のPCで行い，IBサービスの利用はIBサービス専用のPC（以下，IB専用PCという）1台で行っている。

IBサービスにおける情報セキュリティに関する仕様を図1に示す。

(a) IB サービスの利用者登録申請及びログイン

IB サービスを利用する法人は，法人内で IB サービスを利用した事務処理を行う者（以下，利用者という）を書面で C 銀行に登録申請する。利用者は，ログインするとき，利用者ごとに発行された利用者 ID 及びパスワードを入力する。利用者は，IB サービスのパスワード管理メニューでパスワードを変更することができる。

(b) ディジタル証明書

利用者は，ログインするとき，利用者 ID 及びパスワードに加えて，ディジタル証明書を利用する。ディジタル証明書は，C 銀行によって IB サービス利用法人の口座ごとに発行される。IB サービス利用法人には，C 銀行から，①ディジタル証明書と秘密鍵を格納した耐タンパ性をもつ IC カード 1 枚，USB 接続式 IC カードリーダ 1 台及び PC 用 IC カードドライバが，提供される。

なお，PC に接続した IC カードリーダに IC カードを挿入したとき，IC カード利用のための暗証番号を入力する必要がある。暗証番号は IB サービス利用申込時に書面で登録申請する。

(c) 承認ワークフロー

振込の操作は，承認依頼と承認の 2 回の操作に分かれている。承認は承認依頼とは別の利用者でなければ実行できない。ただし，承認依頼の操作で入力された情報は，承認の操作の時に修正できる。

(d) ワンタイムパスワード

利用者は，振込の承認依頼を実行するとき，C 銀行が利用者ごとに提供するワンタイムパスワード生成器（以下，トークンという）が生成するワンタイムパスワードを IB サービスの操作画面に入力する必要がある。

トークンは，トークンごとの秘密情報と時刻情報を基にして，あるアルゴリズムによってワンタイムパスワードを生成しており，IB サービスのサーバも同じ情報とアルゴリズムを使うことによってトークンと同期したワンタイムパスワードを生成する。IB サービスのサーバは，利用者が入力したワンタイムパスワードと，サーバで生成されたワンタイムパスワードを比較して認証する。ワンタイムパスワードは 1 分ごとに更新され，生成された後 2 分間有効である。

(e) トランザクション認証

利用者は，振込の承認を実行するとき，振込先の口座番号をトークンに入力する。トークンは，トークンごとの秘密情報，振込先の口座番号及び時刻情報を基にしてあるアルゴリズムによってワンタイムパスワードを生成する。利用者はそのワンタイムパスワードを IB サービスの操作画面に入力して振込を承認する。

(f) 振込の操作を知らせるメール

(e)の振込の承認が実行されると，振込の承認が実行されたことを知らせるメールが，あらかじめ IB サービスに登録されたメールアドレスに送信される。メールには，振込の承認を実行した利用者 ID，日時などが記載されている。

(g) 履歴の照会

利用者は，IB サービスの履歴照会メニューで，振込内容，承認依頼及び承認を実行した利用者 ID，日時などの履歴を照会することができる。

(h) EV-SSL

IB サービスでは EV-SSL サーバ証明書を採用している。

図 1 IB サービスにおける情報セキュリティに関する仕様（抜粋）

F 社では，経理担当者それぞれに，IB サービスの利用者 ID 及びパスワードが発行され，トークンが提供されている。IC カードは 1 枚を 3 名で共用している。

〔F 社における標準的な振込手続〕

F 社では，自社のサーバで稼働している会計システム（以下，F 社会計システムという）の取引先口座マスタの登録，変更，削除の操作は M 主任が担当している。取引先口座マスタには，取引先の口座情報（金融機関名，支店名，口座種別，口座番号，口座名義人など）が登録されている。F 社における標準的な振込手続を図 2 に示す。

1. 振込依頼情報作成及び依頼書・データ出力

M 主任は，取引先への支払のために振込を行う場合，F 社会計システムを操作して，振込先名，振込先口座情報，振込金額及び振込指定日の情報（以下，この四つの情報を振込依頼情報という）を作成し，振込依頼書として紙に出力する。このとき，取引先口座マスタに登録されている口座情報を利用する。

また，M 主任は，振込依頼情報を C 銀行指定の“振込依頼データ”の形式で出力し，企画管理部の共有フォルダに保存する。

2. 振込依頼書の承認（書類に押印）

L 課長は，請求書など，振込の根拠となる証憑（ショウヒョウ）と振込依頼書を突き合わせて振込依頼情報を確認の上，承認印を押して N さんに回付する。

3. IB サービスでの振込（承認依頼）

N さんは，振込依頼書の記載に従い，IB サービスの操作画面で振込承認依頼を入力する。件数が多い場合は，共有フォルダ上の“振込依頼データ”を IB サービスにアップロードし，振込依頼書の内容と突き合わせて確認する。N さんが承認依頼を実行する。

4. IB サービスでの振込（承認）

M 主任は，IB サービスの操作画面で，振込承認依頼の内容と振込依頼書を突き合わせて確認し，誤りがなければ承認を実行する。これで IB サービスでの振込手続が完了する。振込承認依頼の内容に誤りなどがあれば N さんに差し戻す。又は，M 主任が，②内容を修正して承認を実行することもできる。

5. 振込の記録及び振込依頼書の保管

M 主任は，振込の承認を実行した日付を F 社会計システムの振込依頼情報に追記する。また，振込依頼書を共用キャビネットに保管する。

（“6. 振込完了の確認及び記録”は省略）

図 2　F 社における標準的な振込手続

〔F 社における IB サービス利用時の情報セキュリティリスク及びその対策〕

F 社では，IB サービス利用時の情報セキュリティリスクを想定し，表 1 に示す対策を実施している。

表1　IBサービス利用時の情報セキュリティリスク及びその対策

情報セキュリティリスク	対策
IB専用PCへの不正アクセス	（省略）
IB専用PCのマルウェア感染	・マルウェア対策ソフトのマルウェア定義ファイルを最新化する。 ・［a1］ ・［a2］ ・［a3］
ICカードの盗難，紛失	・利用時以外は，ICカードを経理担当者用の共用キャビネットに施錠保管する。
［b1］	・ICカードの暗証番号を推測されにくいものにする。 ・IBサービスのパスワードを推測されにくいものにする。
［b2］	・トークンを各自のロッカーに施錠保管する。 ・振込の操作を知らせるメールの宛先として，経理担当者3名のメールアドレスを登録する。
［b3］	・振込の操作を知らせるメールの宛先として，経理担当者3名のメールアドレスを登録する。

〔B社からの問合せ〕

10月2日の朝，取引先であるB社の営業担当者から，先月末までに入金予定の商品代金800万円がまだ入金されていないとの電話が入った。応対したL課長は，折返しの返答を約束して電話を切り，Nさんに F 社会計システムの記録を確認させたところ，当該代金は振込済であることが分かった。あいにく M 主任は外出しており不在だったので，L課長は，Nさんに振込の詳細を確認した。次は，Nさんと L 課長との会話である。

Nさん　：IBサービスの履歴も確認しましたが，先月28日に振り込んでいます。

L課長　：振込先誤りの可能性はありませんか。

Nさん　：振込先は振込依頼書どおりでしたが，8月まで利用していた B 社の口座とは違っていました。振込時は L 課長が出張中だったので，振込依頼書の承認は受けずに振込の承認依頼を実行するよう M 主任から直接指示を受けました。IBサービスで私が振込の承認依頼を実行した後，M 主任がそのまま承認しています。

L課長　：M 主任に経緯を確認しましょう。IB専用PCのマルウェア感染も心配です。③振込の操作画面上は正しく操作しているように見えても，銀行との間で

送受信される振込先口座情報をマルウェアが書き換えていたという報道記事を以前読んだことがあります。

夕方，M 主任が外出先から戻ると，L 課長は，B 社から受けた問合せと，振込の詳細について確認した内容を伝えた。

M 主任にも，B 社に入金されていない理由は分からなかった。M 主任によれば，先月末，B 社の経理部長との間で請求書の発行時期や振込期限などについてメールでやり取りをしており，口座変更の連絡と改訂された請求書を受信し，了解の旨を返信した後，お礼を受信してメールのやり取りを終えていた。

M 主任が口座変更の根拠として保管していた B 社の経理部長からのメールを図 3 に示す。

日時　：2018 年 9 月 27 日　16:36
差出人：YYYY <YYYY@interiar-bsha.com>
宛先　：M@f-sha.com
CC　　：ZZZZ@interiar-bsha.com
件名　：Re: Re: 【ご相談】支払条件の件
添付ファイル：　請求書.pdf

M 様
諸々お気遣いいただきありがとうございます。
追加のお願いで申し訳ないのですが，この度，弊社の銀行口座を下記のとおり変更いたしました。月末の急な連絡で誠に恐縮ですが，今月末の入金から，新口座宛てにお振込いただけますでしょうか。
不都合，不明点などありましたらご連絡いただきたくよろしくお願いします。
　新口座
　●●●銀行●●●支店
　普通預金　XXXXXXX
　名義　　ビーシャ
改訂した請求書の写しを添付します。添付ファイルを開封するためのパスワードは前回と同じです。
B 社経理部 YYYY

図 3　B 社の経理部長からのメール

B 社の経理部長からのメールに表示されていたメールアドレスを表 2 に示す。

表２　Ｂ社の経理部長からのメールに表示されていたメールアドレス

役職	最後の２通のメールに表示されていたメールアドレス	普段使われているメールアドレス
Ｂ社の経理部長	YYYY@interiar-bsha.com	YYYY@interior-bsha.com
Ｂ社の社長	ZZZZ@interiar-bsha.com	ZZZZ@interior-bsha.com

早速，Ｍ主任からＢ社の経理部長に確認したところ，Ｂ社は口座を変更しておらず，変更を伝えるメールは送っていないということだった。Ｆ社から第三者の口座に商品代金を振り込んだことが分かったので，Ｆ社は，振込先の銀行に連絡し，事実関係を整理して警察に被害届を提出した。

〔手口と対策〕

後日，警察から，９月末にＢ社を退職した元従業員を被疑者として逮捕し，犯行手口に関する供述を得たとの連絡があった。被疑者の指定した口座に振り込ませるよう，偽メールを送信したとのことであった。被疑者は８月にＢ社の経理部長の手帳からメール受信のためのパスワードを盗み見て以来，職場の自分のＰＣで経理部長のメールを不正に閲覧していた。④Ｂ社の情報システム部が自社のログ収集システムに保管していたログからこのことが分かり，被疑者特定の手掛かりになった。

なお，被疑者は，［　c　］，メールを送っていた。

Ｌ課長は，今回の出来事を教訓としてＦ社で改善すべき点がないか，情報セキュリティリーダであるＳ主任と話し合った。そのときの会話を次に示す。

Ｌ課長　：今後，我が社が偽メールにだまされないための対策はありますか。

Ｓ主任　：第三者によるメールの不正な閲覧への対策にもなるので，できれば取引先に［　d　］を使ってもらいたいと思いますが，同意を得て準備する手間も掛かります。偽メールにだまされないための対策のうち確実であり，かつ，すぐできるものとして，振込に関わるメールのやり取りの際は，［　e1　］のがよいと考えます。そのためには，［　e2　］ことも必要です。

Ｌ課長　：我が社の取引先口座マスタの変更手続と，標準的な振込手続には問題はありませんか。

Ｓ主任　：振込依頼情報の作成前に，Ｍ主任が自分一人の判断で取引先口座マスタ中

の B 社の口座情報を変更できたという問題があります。対策として，［ f1 ］ことを進めます。振込依頼書の承認が省略できたという問題については，［ f2 ］ことを進めます。これによって，振込依頼書の書類を廃止でき，操作結果が社内システムに自動的に記録できるようにもなります。

S 主任は，これらの対策を情報セキュリティ委員会に提案し，対策を実施した。

設問 1　図 1 中の下線①について，C 銀行が，利用者にディジタル証明書と秘密鍵を IB サービスを利用する PC 内のハードディスクに格納させるのではなく，IC カードに格納して提供する目的はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　IB サービスを利用する PC のマルウェア感染による秘密鍵の漏えいリスクを低減するため

イ　ディジタル証明書の更新を不要にするため

ウ　複数枚のディジタル証明書を格納できるようにするため

エ　利用者が，IB サービスの利用者 ID とパスワードを知らなくても，IC カードで IB サービスにログインできるようにするため

オ　利用者が，IB サービスを利用する PC を，複数人で共用できるようにするため

設問2　図2中の下線②について，この段階でM主任が内部不正を働くおそれに対して，内部不正を思いとどまらせるために有効な牽制手段はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　IB専用PCを共用キャビネットに施錠保管し，必要なときだけ取り出して使うルールとする。

イ　L課長が，IBサービスの履歴と振込依頼書を突き合わせて点検し，差があればM主任に理由を聞くルールとする。

ウ　承認の操作の際，急がない修正は，修正して承認を実行する機能を利用せず，差し戻すルールとする。

エ　トークンを共用キャビネットに施錠保管し，使うときだけ貸し出すルールとする。Nさんが共用キャビネットの鍵を管理して貸出記録をつける。

オ　振込先の口座情報はIBサービス画面で手入力せず，“振込依頼データ”をIBサービスにアップロードするルールとする。

設問３　〔F 社における IB サービス利用時の情報セキュリティリスク及びその対策〕について，(1)，(2) に答えよ。

(1)　表 1 中の［ a1 ］～［ a3 ］に入れる，次の (i) ～ (vi) の組合せはどれか。a に関する解答群のうち，最も適切なものを選べ。

(i)　IB 専用 PC では，メール利用を禁止する。

(ii)　IB 専用 PC の OS にログインするには，経理担当者専用の共有アカウントを使う。

(iii)　IB 専用 PC は，社内ネットワークには接続せず，インターネットに直接接続する。

(iv)　IB 専用 PC から社内のファイルサーバへのアクセスは，企画管理部の共有フォルダへのアクセスだけを許可する。

(v)　IB 専用 PC では，使用していない USB ポートを物理的に閉鎖する。

(vi)　プロキシで，社外サイトへのアクセスは OS アップデートとマルウェア定義ファイルのアップデートだけを許可するように設定する。

a に関する解答群

	a1	a2	a3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iv)	(v)
カ	(i)	(iv)	(vi)
キ	(ii)	(iii)	(v)
ク	(ii)	(iv)	(v)
ケ	(ii)	(v)	(vi)
コ	(iv)	(v)	(vi)

(2) 表1中の［ b1 ］～［ b3 ］に入れる，次の (i) ～ (vi) の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

(i) 経理担当者以外の者による，IB サービスへの不正なログイン操作

(ii) 経理担当者が操作を誤ることによる，振込金額や振込先の誤り

(iii) 経理担当者がフィッシングサイトに誘導されることによる，パスワード及び IC カード中の秘密鍵の盗難

(iv) 経理担当者による，自身の利用者 ID を使った不正な振込の承認

(v) 経理担当者の他の経理担当者へのなりすましによる，IB サービスへの不正なログイン操作

(vi) 経理担当者の他の経理担当者へのなりすましによる，又は経理担当者以外の者による，不正な振込の操作

b に関する解答群

	b1	b2	b3
ア	(i)	(iv)	(ii)
イ	(i)	(iv)	(v)
ウ	(i)	(vi)	(iv)
エ	(i)	(vi)	(v)
オ	(iii)	(i)	(iv)
カ	(iii)	(iv)	(v)
キ	(iii)	(vi)	(iv)
ク	(v)	(i)	(iv)
ケ	(v)	(iv)	(ii)
コ	(v)	(vi)	(ii)

設問4　〔B社からの問合せ〕について，(1)，(2)に答えよ。

(1)　本文中の下線③について，このようなサイバー攻撃手法の名称を，解答群の中から選べ。

解答群

ア　CSRF　　イ　DDoS

ウ　MITB　　エ　クリックジャッキング

オ　クロスサイトスクリプティング　　カ　フィッシング

(2)　本文中の下線③について，このようなサイバー攻撃手法への対策として，図1に示す情報セキュリティに関する仕様のうち，最も有効なものを解答群の中から選べ。

解答群

ア　(a)　　イ　(b)　　ウ　(c)　　エ　(d)

オ　(e)　　カ　(f)　　キ　(g)　　ク　(h)

設問5　〔手口と対策〕について，(1)～(5)に答えよ。

(1)　本文中の下線④について，被疑者を特定するために最も有効だったと考えられるものを，解答群の中から選べ。

解答群

ア　B社の経理部長が使っているPCで記録されたメール送受信ログ

イ　B社のメールサーバで記録されたメールクライアントソフトからの大量のログイン失敗ログ

ウ　B社のメールサーバで記録されたメールクライアントソフトからのメール受信要求ログ

エ　B社のメールサーバで記録されたメールクライアントソフトからのメール送信ログ

オ　被疑者が自宅で使っていた個人所有のPCで記録された操作ログ

(2) 本文中の［ c ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

c に関する解答群

ア　B 社から貸与された PC を使い，B 社の経理部長のアカウントを盗用して

イ　B 社から貸与された PC を使い，メールクライアントソフトの設定で差出人メールアドレスを B 社のドメイン名とよく似た実在しないドメイン名に詐称して

ウ　B 社の経理部長が席を外した隙に，B 社の経理部長が使っている PC のメールクライアントソフトを使って

エ　B 社のドメイン名とよく似たドメイン名を取得し，個人所有の PC でメールサーバを立ち上げて

(3) 本文中の［ d ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

d に関する解答群

ア　HTTP over TLS 利用の Web メール

イ　POP before SMTP

ウ　S/MIME によるディジタル署名付き暗号メール

エ　SMTP-AUTH

オ　SPF（Sender Policy Framework）

カ　パスワード付き ZIP ファイル

(4) 本文中の［ e1 ］，［ e2 ］に入れる字句の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

e に関する解答群

	e1	e2
ア	受信メールの差出人メールアドレスと文面を慎重にチェックする	受信メールを印刷して情報セキュリティリーダを含め複数人でチェックする
イ	受信メールの差出人メールアドレスと文面を慎重にチェックする	情報セキュリティリーダに受信メールの写しを転送する
ウ	メールの内容について電話をかけて確認する	振込に関する詐欺事例と振込時の注意事項を経理担当者に教育する
エ	メールの内容について電話をかけて確認する	メールには必ず差出人の電話番号を記載してもらう
オ	メールをサーバに保存しておく	保存用のメールアドレスにもメールを同報する
カ	メールをサーバに保存しておく	保存用のメールアドレスにもメールを同報するとともに，情報セキュリティリーダが必要に応じてメールの内容を確認できる仕組みを作る

(5) 本文中の［ f1 ］，［ f2 ］に入れる，次の (i) ～ (vi) の組合せはどれか。f に関する解答群のうち，最も適切なものを選べ。

(i) F 社会計システムから共有フォルダに出力した後の振込依頼データは L 課長がディジタル署名を付与してから保管する

(ii) F 社会計システムの取引先口座マスタの登録及び変更のワークフローシステムを導入し，その申請権限と承認権限を分離する

(iii) IB サービスでの振込（承認）の承認者を，振込依頼書の承認者と同一人物にする

(iv) IB サービスでの振込の承認を実行する時に，もう一度，取引先の口座情報の変更の証憑と突き合わせて確認する

(v) 取引先口座マスタを登録，変更するときに取引先から入手すべき証憑の種類をマニュアルに明記する

(vi) 振込依頼情報を申請するワークフローシステムを F 社会計システムに導入し，かつ，振込依頼情報の申請権限と承認権限を分離する

f に関する解答群

	f1	f2
ア	(ii)	(i)
イ	(ii)	(iii)
ウ	(ii)	(vi)
エ	(iv)	(i)
オ	(iv)	(iii)
カ	(iv)	(vi)
キ	(v)	(i)
ク	(v)	(iii)
ケ	(v)	(vi)