SG

平成30年度　春期
情報セキュリティマネジメント試験
午後　問題

試験時間	12:30 ～ 14:00（1時間30分）

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3
選択方法	全問必須

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) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B 又は HB の黒鉛筆で答案用紙の**マークの記入方法**のとおりマークしてください。マークの濃度がうすいなど，**マークの記入方法**のとおり正しくマークされていない場合は読み取れません。特にシャープペンシルを使用する際には，マークの濃度に十分注意してください。訂正の場合は，あとが残らないように消しゴムできれいに消し，消しくずを残さないでください。

(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**を記入及びマークしてください。答案用紙の**マークの記入方法**のとおり記入及びマーク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及びマークしてください。

(3) **解答**は，次の例題にならって，**解答欄**にマークしてください。答案用紙の**マークの記入方法**のとおりマークされていない場合は，採点されません。

〔例題〕　次の［　　］に入れる適切な字句を，解答群の中から選べ。

春の情報処理技術者試験は，［ a ］月に実施される。

解答群　　ア　2　　イ　3　　ウ　4　　エ　5

適切な字句は“ウ　4”ですから，次のようにマークしてください。

例題	a	ア	イ	●	エ	オ	カ	キ	ク	ケ	コ

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。

全問が必須問題です。必ず解答してください。

問1　個人情報の保護に関する法律への対応に関する次の記述を読んで，設問1～3に答えよ。

W 社は，ヘルスケア関連商品の個人向け販売代理店であり，従業員数は 300 名である。組織は，営業部，購買部，情報システム部などで構成される。営業部には，営業企画課，及び販売業務を行う第1販売課から第15販売課までがある。

W 社では，5 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（以下，W 社委員会という）を設置した。W 社委員会の事務局は，情報システム部が担当している。また，各部の部長は，W 社委員会の委員及び自部署における情報セキュリティ責任者を務め，自部署の情報セキュリティを適切に確保し，維持，改善する役割を担っている。各情報セキュリティ責任者は，自部署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する。

W 社委員会は，2015 年に改正された個人情報の保護に関する法律（以下，保護法という）への対応の準備を各部で開始することを決定した。これを受けて，営業部では，情報セキュリティリーダである営業企画課の N 課長が，情報システム部の S 課長の支援を得て，保護法への対応の準備を進めることになった。

W 社では，国の個人情報保護委員会が定めた個人情報の保護に関する法律についてのガイドライン（以下，保護法ガイドラインという）のうち，通則編及び匿名加工情報編への対応は必要であるが，それら以外の保護法ガイドラインへの対応が必要な事業は実施していないことを W 社委員会で確認した。また，特定個人情報の取扱いについて検討が必要な場合は，人事担当者などを含めた検討の機会を別途設けることにし，今回の検討範囲からは除外することも W 社委員会で確認した。

〔データベースの項目に関する調査及び検討〕

営業部が主管するデータベース（以下，DB という）のうち，保護法への対応が必要なものには，表1に示す顧客情報 DB 及び表2に示す販売履歴情報 DB がある。N 課長と S 課長は，これらの DB に格納されているデータを調査した。

表 1　顧客情報 DB の項目及びデータ型

項番	項目	データ型
1	顧客番号	整数
2	氏名	文字列
3	性別	文字列
4	住所	文字列
5	生年月日	日付
6	肌質	文字列 [1]

注 [1]　肌質を数十種のカテゴリに分類し，それぞれに応じた記号や名称を使う。例えば，乾燥肌であれば程度に応じて“K001”～“K100”のような記号を，アトピー性皮膚炎であれば“ATPD”のような名称を使う。

表 2　販売履歴情報 DB の項目及びデータ型

項番	項目	データ型
1	顧客番号	整数
2	販売番号 [1]	整数
3	販売年月日	日付
4	商品コード	文字列
5	販売数量	整数

注 [1]　複数の商品を 1 注文で同時に販売した場合は，同じ販売番号が振られる。また，販売番号は販売が行われるたびに，1 ずつカウントアップされる。

N 課長と S 課長は，この調査結果を踏まえ，保護法及び保護法ガイドラインに基づき対応を検討した。次はそのときの会話である。

N課長：肌質という項目には，アトピー性皮膚炎などの病歴が分かる名称が記録されている場合があります。病歴は，保護法に定められているように本人に対する不当な差別，偏見その他の不利益が生じないように，［　a　］として特に注意して取り扱わなければいけません。

S 課長：［　a　］とそれ以外の個人情報とは，取扱いはどのように違うのですか。

N課長：幾つか違いがあります。例えば，保護法及び保護法ガイドラインによれば，［　a　］以外の個人情報が記載された書面を本人から直接取得する場合は，利用目的の［　b　］が必要ですが，［　a　］を取得する場合は，取得することについて本人の［　c　］を得ることも必要です。ただし，幾つか注意すべき事項があります。ここでは，二つ説明します。

一つ目は，本人から適正に直接取得する場合です。その場合は本人が提供

したことをもって［ c ］を得たと解されます。

二つ目は，法令に基づき取得する場合です。例えば会社が［ d ］に基づき従業員の健康診断を実施し，病状，治療などの情報を健康診断実施機関から取得するときは，本人の［ c ］を得ることは不要です。

〔PC に関する情報セキュリティ対策の検討〕

営業部で使用する機器は，オフィスに設置したサーバ，デスクトップ PC（以下，DPC という），電話，ファックスなどである。サーバには，顧客情報 DB 及び販売履歴情報 DB，並びに提案書ひな形などの共有ファイルを格納している。サーバのデータのバックアップは，外部記憶媒体に格納し，キャビネットに保管している。

W 社の営業スタイルは，主として訪問販売であり，紙媒体による提案資料の提示や多数のサンプル品の持参など，旧態依然としたものである。そこで，営業部長は，売上拡大を図るために，営業スタイルの見直しと効果的なマーケティング計画の立案を N 課長に指示した。

営業スタイルについては，N課長は，モバイル PC（以下，MPC という）を活用することによって見直しをすることにした。MPC には SFA（Sales Force Automation）ツールを導入し，訪問先でも在庫確認処理，受発注処理などを行えるようにする。

N 課長は，自社の営業部員が初めて MPC を携行することになることから，他社で発生した MPC の紛失・盗難などの情報セキュリティ事故を踏まえた情報セキュリティ対策を検討する必要があると考えた。そこで，S 課長の協力を得て，MPC に関する情報セキュリティ対策を表 3 のとおりまとめて W 社委員会に諮り，承認を得た。

表 3　MPC に関する情報セキュリティ対策

目的	情報セキュリティ対策
1. MPC の紛失・盗難そのものを防止	・①営業部員が MPC を携行する際の紛失・盗難そのものを防止するための順守事項の周知徹底
2. MPC 内ハードディスクに保存された情報の漏えいを技術的に防止	・外部記憶媒体から MPC を起動できない設定の実施 ・ハードディスクを抜き取られてもデータを読み取られないように，自動的に暗号化を行うハードディスクを内蔵した MPC の採用
3. 紛失・盗難中における情報漏えいの可能性について，回収後の MPC を確認	・OS コマンドを使われた可能性や SFA ツールを迂回された可能性があるとの前提で，②MPC 内のファイルが読み取られた可能性が低いことを確認できる機能の組込み

N課長は，DPCからのファイルの持出し，訪問先で更新したファイルのDPCへの取込みなどを迅速かつ確実に行うためのツールの要件を検討した。この要件をS課長に提示し，要件の実現方法の検討並びにツールの開発及び導入を依頼した。S課長は，検討の後，依頼どおりツールを開発し，導入した。

さらに，N課長は，個人データの漏えい，滅失又は毀損が起こった場合を想定し，国の個人情報保護委員会が定めた“個人データの漏えい等の事案が発生した場合等の対応について”の告示に基づき，③国の個人情報保護委員会などに対して速やかに報告するように努めるべきとされている場合を明らかにし，社内規程に盛り込んだ。

〔マーケティング計画の立案の検討〕

効果的なマーケティング計画の立案については，N課長は，顧客情報や販売履歴情報を分析し，顧客特性や販売チャネルなどに応じたマーケティングを検討することにした。

Z社は，様々な業界のデータを保有するDB提供会社である。W社はZ社に販売履歴に関するデータを提供し，Z社からはW社と同じ業界及び他業界のデータも含めた分析結果を受領することにした。これによって，W社は，顧客特性に即した商品を提案できるようになり，販売活動の効率化が期待できる。

N課長は，1か月分の販売履歴情報DB及び当該月末時点の顧客情報DBのデータを併合し匿名加工情報に加工したものを，翌月10日までにZ社に提供することにした。

N課長は，匿名加工情報に加工する方法について，S課長に検討を依頼しており，本日，N課長はS課長から報告を受けた。次はそのときの会話である。

S課長：検討の結果，匿名加工情報に加工できる目途がつきました。特定の個人を識別できる情報から，氏名は削除し，住所は記述の一部を削除します。また，極端に販売数量が大きい注文の販売履歴情報については，販売数量をあらかじめ定めた上限値に置き換えます。必要に応じて他の加工も行います。

N課長：分かりました。ただし，④当社のマーケティングに有効な分析ができる匿名加工情報であることが必要です。実施する分析は，“商品ごとの同時に購入

される他の商品の傾向の分析”，“年齢層ごとの年間を通じた売れ筋商品の傾向の分析”，“新商品ごとの発売開始後の月別販売数量推移と肌質との相関関係の分析”，“商品ごとの性別と年間販売数量との相関関係の分析”です。

S課長：分かりました。それらの分析ができるように工夫します。ところで，Z社に匿名加工情報を取り扱ってもらう際に，注意してもらわなければならないことはありますか。

N課長：保護法には⑤義務規定があるので注意する必要があります。ですが，Z社はコンプライアンス体制が整備されているので，当然理解していると考えられます。

N課長は，営業部長の指示を実行し，半年後には，売上も対前年比で好調に推移し始めた。営業部長は，N課長の一連の取組みの成果を高く評価した。

設問1　本文中の［　a　］～［　d　］に入れる字句はどれか。それぞれの解答群のうち，保護法及び保護法ガイドラインに基づいたときに，最も適切なものを選べ。

aに関する解答群

ア　営業秘密　　イ　機微情報　　ウ　個人データ
エ　センシティブ情報　　オ　保有個人データ　　カ　要配慮個人情報

bに関する解答群

ア　開示　　イ　公表　　ウ　主張
エ　通知　　オ　提示　　カ　明示

cに関する解答群

ア　回答　　イ　共感　　ウ　信頼
エ　同意　　オ　認識

dに関する解答群

ア　次世代育成支援対策推進法　　イ　賃金の支払の確保等に関する法律
ウ　労働安全衛生法　　エ　労働基準法
オ　労働組合法　　カ　労働契約法

設問２　〔PC に関する情報セキュリティ対策の検討〕について，(1) ～ (3) に答えよ。

(1)　表 3 中の下線 ① について，次の (i) ～ (vi) のうち，有効な順守事項だけを全て挙げた組合せを，解答群の中から選べ。

(i)　BIOS パスワードなど電源起動時のパスワードを設定した MPC を携行する。

(ii)　MPC の液晶画面にのぞき見防止フィルタを取り付ける。

(iii)　MPC を携行しているときは，酒宴に参加しない。

(iv)　移動中，電車の中で，MPC を網棚に置かない。

(v)　営業車から離れるときは，短時間でも車両内に MPC を放置しない。

(vi)　ハードディスクのデータをリモートで消去できる機能をもつ MPC を携行する。

解答群

ア　(i)，(ii)，(iii)　　イ　(i)，(ii)，(vi)　　ウ　(i)，(iii)，(iv)

エ　(ii)，(iii)，(iv)　　オ　(ii)，(iii)，(iv)，(v)　　カ　(ii)，(iv)，(vi)

キ　(ii)，(vi)　　ク　(iii)，(iv)　　ケ　(iii)，(iv)，(v)

コ　(v)，(vi)

(2)　表 3 中の下線 ② について，確認できる機能を二つ，解答群の中から選べ。

解答群

ア　MPC 起動時の BIOS 設定など，OS 立上げ前の段階で，利用者が設定するパラメタと，管理者権限をもつ者が設定するパラメタとを分離する機能

イ　MPC 内のファイルへのアクセスについてのログを取得し，そのログの参照，変更，消去の権限を利用者に付与する機能

ウ　OS へのログインの成功時に，MPC に搭載されたカメラを使って操作者の写真を撮り，またその画像の更新や消去には管理者権限を必要とする機能

エ　OS へのログインの成否をログに記録し，そのログの消去には管理者権限を必要とする機能

オ　SFA ツールへのログインの成否をログに記録し，そのログの消去には管理者権限を必要とする機能

(3) 本文中の下線③について，次の(i)～(v)のうち，該当する場合だけを全て挙げた組合せを，解答群の中から選べ。

(i) 宛名及び送信者名だけの個人データが含まれている文書を，相手先のファックス番号を間違えて，他の会社に送信した場合

(ii) 火災に遭い，顧客情報DBを格納したサーバのハードディスクが焼損し，顧客情報DBがバックアップも含め全て滅失した場合

(iii) 顧客情報DBのデータ全てを印刷した顧客リストを紛失し，漏えいは確認できていないものの，そのおそれがある場合

(iv) 高度な暗号化を施した顧客情報DBのデータを，委託先である印刷会社に送信しようとしたが，誤って別の会社に送信した場合

(v) システムへの登録前の顧客情報登録用シートを，顧客の氏名の五十音順に重ねて置いていて盗難に遭った場合

解答群

ア (i)	イ (i)，(ii)	ウ (i)，(iii)
エ (i)，(iii)，(iv)，(v)	オ (i)，(iii)，(v)	カ (ii)
キ (ii)，(iii)	ク (iii)	ケ (iii)，(v)
コ (iv)，(v)		

設問３　〔マーケティング計画の立案の検討〕について，(1)，(2) に答えよ。

(1)　本文中の下線 ④ について，次の (i) ～ (vi) のうち，匿名加工情報に加工する適切な方法を四つ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

(i)　顧客番号について，乱数などの他の記述を加えた上で，ハッシュ関数を使って変換する。

(ii)　生年月日について，月日を削除して生年だけにする。

(iii)　性別を削除する。

(iv)　肌質について，特異なケースを除外するために，あらかじめ定めたしきい値よりも該当レコード数が少ない病歴の場合は，当該レコードを削除する。

(v)　販売年月日について，日を削除して販売年月だけにする。

(vi)　販売番号について，１の位を四捨五入したものにする。

解答群

ア　(i)，(ii)，(iii)，(iv)　　イ　(i)，(ii)，(iv)，(v)

ウ　(i)，(ii)，(v)，(vi)　　エ　(i)，(iii)，(iv)，(v)

オ　(i)，(iii)，(iv)，(vi)　　カ　(i)，(iii)，(v)，(vi)

キ　(i)，(iv)，(v)，(vi)　　ク　(ii)，(iii)，(iv)，(v)

ケ　(ii)，(iv)，(v)，(vi)　　コ　(iii)，(iv)，(v)，(vi)

(2) 本文中の下線⑤について，次の (i) ～ (vi) のうち，Z 社が保護法に定める努力義務規定以外の義務規定に違反するおそれがあるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) 複数の会社（W 社及び W 社以外の会社）から受領した匿名加工情報と気象情報との相関を取って，新たな統計情報として作成し，販売した。

(ii) 複数の会社（W 社及び W 社以外の会社）から受領した匿名加工情報へのアクセス権の設定などの安全管理措置を講じたにもかかわらず，その措置の公表を正当な理由なく 1 年を超えて怠った。

(iii) 元の本人を識別するために，W 社から受領した匿名加工情報と，他の会社から受領した情報との照合を行ったところ，数百件程度，識別に成功した。

(iv) 元の本人を識別するために，W 社から受領した匿名加工情報と，他の会社から受領した情報との照合を試みたが，結果は全て失敗した。

(v) 元の本人を匿名加工情報から識別するために，書面での秘密保持契約を交わした上で，W 社が用いた加工方法を，W 社から有償で取得した。

(vi) 元の本人を匿名加工情報から識別するために，書面での秘密保持契約を交わすことなく，口頭での合意の上で，W 社が用いた加工方法を，W 社から無償で取得した。

解答群

ア (i), (ii), (iii)　　イ (i), (ii), (iii), (iv)

ウ (i), (ii), (iii), (iv), (v)　　エ (i), (iii), (iv), (v), (vi)

オ (i), (iii), (vi)　　カ (ii), (iii), (vi)

キ (iii), (iv), (v), (vi)　　ク (iii), (iv), (vi)

ケ (iii), (vi)　　コ (v), (vi)

問２　内部不正事案に関する次の記述を読んで，設問１，２に答えよ。

Q 社は，従業員数 300 名の保険代理店であり，生命保険会社 2 社，損害保険会社 2 社と代理店委託契約を締結し，保険商品を販売している。Q 社の主な組織，担当業務及び体制を表１に示す。

表１　Q 社の主な組織，担当業務及び体制

組織		担当業務	体制
本社	総務部	総務，経理，人事，情報システム管理など	部長：1 名 主任：2 名，スタッフ：7 名
	営業部	販売制度企画，営業所管理・支援，顧客管理，市場調査など	部長：1 名 主任：4 名，顧客管理スタッフ：3 名 その他スタッフ：12 名
営業所 1)		保険の代理店販売（首都圏に 5 か所）	所長：1 名 主任 2)：3 名，営業担当者：45 名 スタッフ：3 名

注記　営業所の所長と主任を併せて，営業所管理者という。
注 1)　営業所は，営業部の管轄である。また，営業所の体制欄の人数は，T 営業所の例を示す。
2)　営業所の各主任は，通常，営業担当者 10～20 名のチームを所管している。

Q 社では，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（以下，Q 社委員会という）を設置して，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定めている。総務部長，営業部長は Q 社委員会の委員であり，総務部長は総務部の，営業部長は営業部及び全営業所の情報セキュリティ責任者である。また，総務部で，総務及び情報システム管理の業務を担当している G 主任は，総務部の情報セキュリティリーダであり，営業部で，営業所管理・支援業務を担当している H 主任は，営業部及び全営業所の情報セキュリティリーダである。

Q 社の情報セキュリティ関連規程では，役職，職務などに応じて，アクセス可能なデータの範囲及び情報システムの操作権限を適切に設定することを求めている。

営業担当者が，保険商品の説明資料や提案書を顧客に渡す方法には，“面会して直接手渡す”，“郵送する”，“電子メール（以下，メールという）に添付して送信する”の 3 通りがある。最近は面会が少なくなり，メールに添付して送信することが大半を占めている。Q 社が導入しているメール管理ツールの機能を図１に，メール利用ルールを図２に示す。

・社外送信メールの一時保留機能 1)
・社外送信メールの上長への Bcc による自動送信機能
・社外送受信メールの送信者，日時，宛先，件名，メール本文，添付ファイルなどをメールサーバに自動保存する機能
・保存されているメールの情報の検索，閲覧機能
・メール利用状況のレポート作成機能

注 1) 送信ボタンが押されても，即時送信せずに送信トレイに格納し，送信トレイが送信者によって開かれて確認ボタンが押されると送信する機能

図 1 メール管理ツールの機能（抜粋）

・社内外を問わず，私的なメールを送信してはならない。
・社外にメールを送信する場合，送信者は送信トレイを開いて，一時保留されたメールの宛先，件名，メール本文，添付ファイルがある場合はその内容を確認し，確認ボタンを押さなくてはならない。
・秘密情報は，原則社外に送信してはならない。業務上必要な送信の場合は，事前に上長の承認を得てから，秘密情報を暗号化した上で送信しなければならない。
・上長は，Bcc で届いた社外送信メールを確認しなければならない。暗号化されている場合，上長は，宛先と件名を見て，必要に応じて送信者に内容を確認する。

図 2 メール利用ルール（抜粋）

Q 社では，ここ数年，売上向上や事務作業効率化を目指して，業務のシステム化を推進している。その一環として，各営業担当者が担当している顧客及び見込客の個人情報（以下，顧客情報という）をデータベース化して一元的に管理する顧客情報管理システム（以下，顧客システムという）を 2017 年 4 月 3 日に利用開始することにした。顧客システムは，営業担当者と営業所管理者が顧客情報を共用し，顧客及び見込客に対して最適な保険商品を迅速に提案することを目的の一つにしている。顧客システムの概要を図 3 に示す。

1. 管理する顧客情報
   氏名，性別，生年月日，自宅住所，電話番号，メールアドレス，家族構成，応対履歴などの秘密情報
2. 機能
   ・顧客情報の登録，参照，更新，削除，検索，PC へのダウンロード，印刷など
   ・利用者の管理
3. 利用者とそのアクセス可能範囲
   営業担当者：自らが担当している顧客情報
   営業所管理者：自らが所属する営業所が担当している全顧客情報
   営業部の顧客管理スタッフ：Q 社が担当している全顧客情報
4. 利用者認証方式
   利用者ごとに割り当てた利用者 ID と，利用者が設定したパスワードを使用

図 3 顧客システムの概要

顧客システムは，総務部と営業部の従業員の一部で編成された開発チームが，ベンダの協力を得ながら開発した。2016年10月から3か月間，顧客情報の登録業務などの機能及びユーザビリティの最終確認のために，T営業所で，顧客システムを試行運用した。試行期間中の主な実施事項を次に示す。

・営業所の営業担当者全員及び営業所管理者，営業部の顧客管理スタッフ並びに開発チームのメンバ（以下，試行利用者という）に，試行用の利用者IDを付与
・営業担当者全員は，自らの顧客情報を登録し，図3の機能を確認
・営業所管理者及び営業部の顧客管理スタッフは，図3の機能を確認
・開発チームのメンバは，利用者管理機能，顧客情報のダウンロード機能などを確認

試行終了時に，開発チームは，試行利用者全員に対して，ダウンロードした顧客情報（以下，顧客ファイルという）をPCから削除するように連絡し，試行用の利用者IDを削除した。

〔内部不正事案の発生〕

2017年3月1日にT営業所のK所長から，総務部の人事担当の主任と，営業部H主任に連絡があった。T営業所のJ主任が3月31日付で退職したいと申し出たということであった。J主任の退職届を3月6日に受理したという連絡が人事担当の主任からあり，H主任は，従業員退職時の点検手続に従って，J主任が退職申出日の1か月前からこれまでに社外に送信したメールをチェックした。Q社では，情報セキュリティ関連規程で会社の秘密情報の社外持出しを原則禁止するとともに，万一持ち出したものがあれば全て返却した旨を退職者に退職時の誓約書で誓約させている。

チェックの結果，J主任の私用と思われるメールアドレス宛てに，ファイルが5回送信されていることが分かった。送信されたファイルは，暗号化されていた。H主任は，分かったことをすぐに営業部長に報告した。営業部長は，総務部長及びK所長に連絡し，H主任とともにT営業所に赴いた。営業部長とK所長は，J主任に面談して事情を確認した。その後，営業部長は，K所長とも面談した。J主任との面談結果を図4に，K所長との面談結果を図5に示す。

1. 宛先と送信したファイル

宛先のメールアドレスは，J主任の私用のメールアドレスであり，J主任が送信したファイルは，顧客システムの試行期間中，J 主任が会社の PC に保存した顧客ファイルである。試行終了時に，会社の PC から削除するよう指示があったが，J 主任は削除しなかった。ファイルは自宅の PC に保管している。

2. 私用のメールアドレス宛てに顧客ファイルを送信した理由，状況

J主任は，次のように考えた。

・試行期間中にT営業所で担当している全顧客情報が顧客システムに登録されたが，その中には自分が担当する顧客の情報も多くあるので，退職後ももっていても構わない。

・同業他社に転職したときに，営業所の全顧客情報を利用して営業で良い成績を上げたい。

・登録された顧客情報を利用することはQ社に迷惑を掛けるようなことではないし，後ろめたいようなことでもない。

・K 所長は外回りなどで多忙なので，メールの確認は余りしていないようであり，またスタッフも様々な事務で忙しそうであったので，見つかりはしない。

3. 退職理由など

他チームの営業成績が良い中で，自分のチームだけノルマが達成できず，J 主任は孤独を感じていた。今の状況では自分の実力を発揮できず公平に評価もされないが，同業他社に転職すればもっと実力を発揮でき，評価されると考えた。ただし，他社との雇用契約は未締結。

図4　J主任との面談結果（抜粋）

1. J主任の状況など

K 所長は，主任全員と毎週打合せを行い，また営業担当者とも年数回，面談している。J 主任のチームの成績が伸び悩んでいたので叱咤激励することはあったが，J 主任が思い詰めているようには見えなかった。

2. 管理業務

以前は，営業所にいる時間も確保できて，点検や確認などの管理業務をK所長自身が行っていたが，最近は他社との競争が厳しく，K 所長も積極的に顧客を訪問し，管理業務はできる限りスタッフに任せていた。現在の状況では，メールの上長確認を含め，管理業務に所長が時間を費やし過ぎていると，業績目標の達成は難しいとも考えていた。

3. 教育など

K 所長は，朝礼などで，営業担当者には適切な情報管理を指導している。ただし，実際，どこまで徹底できているか不安を感じている。H 主任も年に数回，営業所に来て営業担当者への情報セキュリティ教育を実施してくれたが，教育後の営業担当者の様子からは，今のやり方では限界があるとK所長は感じている。

顧客システムの試行終了時に，顧客ファイルを PC から消去するよう，開発チームから連絡があり，K所長からも営業所内に周知したが，K所長は試行利用者のPCの中までは点検しなかった。

図5　K所長との面談結果（抜粋）

営業部長は，社長及び Q 社委員会の委員に一報するとともに，各保険会社に対しても状況を報告した。また，営業部長は，総務部長及び弁護士とも相談して，K所長とH主任に，J主任の自宅を訪問し，後日の調査への備え及び顧客情報保護のために，

J 主任の自宅の PC を会社で預かってくるよう指示した。訪問時は，セキュリティ専門事業者の情報処理安全確保支援士（登録セキスペ）である U 氏にも同行を依頼した。

J 主任の自宅で，U 氏が確認したところ，メールで送信された顧客ファイルは自宅の PC に保存されていた。K 所長は，J 主任の同意を得て，自宅の PC を当面，会社で預かることにした。また，面談結果は事実に相違ないこと，顧客情報を業務外で利用していないこと，Q 社から持ち出した顧客情報が他に残っていないか改めて確認し，残っていたら直ちに削除することなどについて J 主任から念書をとった。

営業部長及び総務部長（以下，両部長という）は，今回発生した内部不正事案（以下，事案という）について，3 月 13 日に臨時に開催された Q 社委員会に報告した。また，両部長は，個人情報の保護に関する法律，保険業法，各保険会社との契約などへの対応，社内規程に基づいた J 主任に対する処分と法的措置について，弁護士と相談の上，対応していくことを報告した。Q 社委員会では，CISO が両部長に，メールによる顧客ファイルの不正な送信が他にないか調査すること，及び事案の原因分析と再発防止策の検討を早急に行うことを指示した。これらが完了するまで，2017 年 4 月に予定していた顧客システムの全社での利用開始を延期することにした。また，Q 社委員会では，翌 3 月 14 日に，Q 社の秘密情報の取扱いルール，メール利用ルールなどについて，全従業員に緊急に再周知するとともに，同日分から当面の間，社外送信される全メールについて，メール管理ツールを使って監視を行うよう総務部長に指示した。総務部長は，社外送信メールの上長確認を，当面全件行うように社内に周知した。

〔事案のメール調査〕

Q 社委員会の翌日，両部長は，H 主任と G 主任（以下，両主任という）に，顧客情報をダウンロードして社外に送信した者が J 主任以外にいないかの調査と，事案の原因分析を指示した。

両主任は，社外送信メールの調査範囲として，対象期間を［ a ］，対象者を［ b1 ］，［ b2 ］に設定した。調査の結果，顧客ファイルの不正送信はなかったが，自宅に仕事を持ち帰るために，私用のメールアドレス宛てに業務関係のファイルを送信している事例が発見された。

〔事案の原因分析〕

両主任は，事案発生までの顧客システムやメールの取扱い，J主任及びK所長との面談結果から，“不正のトライアングル”を基に，表2のとおり，J主任の立場から見た事案の原因を整理した。また，事案発生までのQ社の状況を確認するために，IPAの“組織における内部不正防止ガイドライン（第4版）”を基に，表3のとおり，原因を整理した。

表2　“不正のトライアングル”を基にした原因の整理

項番	要因	事案の原因
1	動機・プレッシャ	・［　c　］ （省略）
2	機会	・顧客システムから顧客情報を大量にダウンロードできたこと ・メールに顧客ファイルを添付して，私用のメールアドレス宛てに送信できたこと ・［　d　］ ・［　e　］ （省略）
3	正当化	・［　f　］ （省略）

注記　要因の分類は，米国の組織犯罪研究者ドナルド・R・クレッシーによる。

表3　“組織における内部不正防止ガイドライン（第4版）”を基にした原因の整理（抜粋）

項番	観点	事案の原因
1	基本方針[1)]	・［　g　］
2	人的管理	・［　h　］
3	職場環境	・［　i　］

注[1)]　経営者の責任の明確化，統括責任者の任命，体制構築が含まれる。

両主任によるメール調査と原因分析の結果は，3月29日に両部長に報告され，両部長は再発防止策の検討を，開発チーム，両主任などに指示した。

〔事案の再発防止策の策定〕

開発チームでは，顧客システムからの顧客情報のダウンロードについて，抽出件数に上限を設けるという対応策を考えた。また，顧客ファイルの保管場所や保管期間に

ついても案を検討した。

営業所管理者によるメールの確認が不十分であるという問題については，総務部が，個人別の社外送信メール数，送信時刻などを監視するとともに，監視について従業員全員に周知する案をまとめた。

再発防止策の案が固まり，両部長は，Q社委員会にメール調査結果，原因分析結果，及び再発防止策の案を報告し，了承された。Q社委員会の報告を受けた社長は，全営業所長と面談した上で，営業所の管理業務全般の見直しを取締役会に提案し，併せて営業所管理者に対する教育にも力を入れることにした。

Q社では，営業所の管理体制の強化及び全従業員への教育も含めた再発防止への取組みを進めた。2017年6月にはその取組みの成果が確認できたので，Q社委員会の承認の下，2017年7月に全社で顧客システムの利用を開始した。

設問1　〔事案のメール調査〕について，(1)，(2)に答えよ。

(1)　本文中の［　a　］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。

aに関する解答群

ア　2016年10月1日から12月31日まで

イ　2016年10月1日から2017年3月6日まで

ウ　2016年10月1日から2017年3月13日まで

エ　2016年10月1日から2017年3月31日まで

オ　2017年1月1日から3月6日まで

カ　2017年1月1日から3月13日まで

キ　2017年1月1日から3月31日まで

(2) 本文中の［ b1 ］，［ b2 ］に入れる字句の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

b に関する解答群

	b1	b2
ア	T 営業所の営業担当者	営業部の顧客管理スタッフ
イ	T 営業所の営業担当者	営業部の顧客管理スタッフ及び開発チームのメンバ
ウ	T 営業所の営業担当者	営業部の全員
エ	T 営業所の営業担当者及び営業所管理者	営業部の顧客管理スタッフ
オ	T 営業所の営業担当者及び営業所管理者	営業部の顧客管理スタッフ及び開発チームのメンバ
カ	T 営業所の営業担当者及び営業所管理者	営業部の全員
キ	T 営業所の全員	営業部の顧客管理スタッフ
ク	T 営業所の全員	営業部の顧客管理スタッフ及び開発チームのメンバ
ケ	T 営業所の全員	営業部の全員

設問2　〔事案の原因分析〕について，(1)，(2)に答えよ。

(1)　表2中の［ c ］～［ f ］に入れる字句はどれか。解答群のうち，最も適切なものをそれぞれ選べ。

c～fに関する解答群

ア　Q社が，自分のことを公平に評価してくれないので，営業成績を悪化させて損害を与えたいと考えたこと

イ　T営業所が担当する顧客情報には，自分が担当する顧客の情報も多くあり，退職後ももっていても構わないと考えたこと

ウ　営業所長が多忙で，不在なときが多く，メールの確認が十分に行われていなかったこと

エ　顧客情報を持ち出して利用すれば，転職先で実力が発揮できて高く評価されると考えたこと

オ　顧客ファイルを会社のPCに保管し続けることができたこと

(2)　表3中の［ g ］～［ i ］に入れる字句はどれか。解答群のうち，最も適切なものをそれぞれ選べ。

g～iに関する解答群

ア　営業所ごとの個別の情報セキュリティリーダの任命・配置が未実施

イ　営業所長が多忙で，不在なときが多く，営業所内のコミュニケーションが不十分

ウ　社外送信メールの記録と保存が不十分

エ　社内の懲戒処分を含めた内部規程及びメール利用ルールなどの周知，教育が不十分

オ　従業員退職時の点検手続及びチェックが不十分

カ　内部不正事案発生時の報告体制及び調査のための備えが不十分

キ　本社において，情報セキュリティ責任者及び情報セキュリティリーダが不足

問３　企業統合における情報セキュリティガバナンスに関する次の記述を読んで，設問１～３に答えよ。

X 社は，本社の他に 20 か所の地方営業所（以下，営業所という）を有する，法人向けオフィス機器などの販売代理店業を営む非上場会社で，従業員数は 320 名である。従業員のうち営業に従事する者（以下，営業員という）は 200 名である。X 社は，旧 X 社が同業で業績が低迷していた旧 Y 社を，販路拡大のために，2016 年 4 月 1 日に吸収合併してできた。

X 社の社長は，合併直後，株式の上場，取引先からの信頼の維持・向上及び事業継続性の向上のために，全社的な業務の効率化，コーポレートガバナンスの強化及び社内の情報システムの計画的な統合を図ることを社長方針として周知した。社長方針を実行に移すために，社長直下に経営企画室を設置し，IT に詳しい C 氏を室長に任命した。コーポレートガバナンスの強化の一環として，情報セキュリティガバナンスを整備するために，社長を委員長，経営企画室を事務局とし，各部室長を委員とする情報セキュリティ委員会（以下，委員会という）を設置した。また，経営企画室の職務分掌には，全社的な情報システムの企画及び運用を含めた。A 部長が率いる営業統括部では，全社的な営業戦略の策定及び営業管理を行っている。営業統括部には管理課がある。管理課の B 課長は，委員会の指示の下，営業部門全体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である。

営業所数は，旧 X 社が 15，旧 Y 社が 10 であったが，合併後，統廃合によって旧 X 社が 14，旧 Y 社が 6 の計 20 となった。合併時点で，旧 Y 社からの事業の承継に伴い提供された顧客データを含め，X 社の顧客データベースに登録されている顧客企業の購買担当者数は 2,800 名となった。

X 社では，全ての営業所に LAN 環境が整備されている。各営業所の従業員は，会社貸与のデスクトップ PC（以下，業務 PC という）を LAN 環境に接続して使用している。本社と各営業所の LAN の間は，WAN 回線で結ばれ，本社においてインターネットに接続している。旧 X 社及び旧 Y 社（以下，両社という）での業務用 IT ツールの利用方法を表 1 に，2016 年 3 月末時点での旧 X 社の情報セキュリティポリシ（以下，情報セキュリティポリシをポリシという）を図 1 に示す。

表1　両社での業務用 IT ツールの利用方法

	営業支援ツール利用	PC 管理	業務用の電子メール（以下，電子メールをメールという）利用
旧 X 社	・SaaS を顧客管理，案件管理などに利用 ・Web ブラウザからアクセスして利用	・PC 管理ツールを利用して，業務 PC の利用者の操作履歴を収集	・業務 PC 上で，氏名検索機能付きメールアドレス帳（以下，メールアドレス帳という）及び宛先入力自動補完機能付きメールクライアントソフトを利用 ・従業員ごとに異なる業務メールアドレスを利用 ・社外からは利用不可
旧 Y 社	・専用ツールは未導入 ・顧客管理は，営業員の業務 PC 上の表計算ソフトで行い，案件報告は口頭又はメールで実施	・ツールは未導入	・Web ブラウザからアクセスして利用 ・従業員ごとに異なる業務メールアドレスを利用 ・社外からは利用不可

1. 業務では，PC，USB メモリ，携帯電話などの機器は会社貸与のものを利用すること
2. 個人情報などの機密性が高い情報は，暗号化，パスワードなどによって保護すること
3. 個人情報などの機密性が高い情報を社外に持ち出す場合には，事前に上長又は所属部門の情報セキュリティリーダの承認を得ること
4. パスワードは，英大文字，英小文字，数字，記号の全ての文字種を組み合わせた 8 文字以上で，かつ，他人に推測されにくい文字列とし，他人に知られないよう管理すること

図1　旧 X 社のポリシ（抜粋）

ポリシは旧 X 社だけが整備していた。旧 X 社のポリシを旧 Y 社の営業所へ適用する時期については，経営企画室が検討し，委員会に諮ることにした。そこで，C 室長は，情報資産の特定及びリスクアセスメントを 2016 年 5 月中旬から開始し，現状の情報資産の取扱状況及び情報セキュリティ対策を調査したところ，同年 6 月中旬に，旧 X 社と比べて旧 Y 社の営業所での情報資産の取扱いがずさんなことが明らかになった。

〔情報システムの利用の変化〕

X 社では，旧 X 社で導入済みの営業支援ツールの利用を 2016 年 7 月から全社的に開始した。同年 8 月からは，業務用のメール利用も旧 X 社で導入済みの方法に全社で統一し，メールの添付ファイルのサイズを 5M バイト以下とする設定にした。同時に，毎年，社外への送信メールを監査することにし，監査証跡として 1 年間分の送信メールを残すために，メールアーカイブサーバをメールサーバとは別に設置した。

経営企画室が，2016 年 9 月に合併後の従業員満足度及び旧 X 社のポリシの全社適用についての社内アンケートを行った。その結果，旧 Y 社の営業員から，不慣れな業務用 IT ツールの利用による勤務時間の増加に対する不満，及び旧 X 社のポリシを全社に適用する方針についての反発が多いことが分かった。そこで，旧 X 社のポリシの適用は，旧 Y 社の営業所では，条文によって時期を分け，2016 年 10 月から 1 年掛けて段階的に行う方針を委員会で決定した。

段階的なポリシの適用を進めていたところ，2015 年に改正された個人情報の保護に関する法律の全面施行日を 2017 年 5 月 30 日とする政令が，2016 年 12 月 20 日に閣議決定された。X 社が取り扱う個人情報は，合併以降 2016 年 12 月 20 日まで 3,800 件を超えることはなかったが，①改正法の全面施行日以降は，X 社も，個人情報取扱事業者に該当することになる。そこで，委員会では方針を変更し，2017 年 1 月 10 日に，旧 X 社のポリシを 2017 年 4 月 1 日から全社適用することにした。社長から経営企画室及び管理課（以下，両課室という）に対して，旧 X 社のポリシの全社適用と社長方針の具体的推進を行うよう指示があった。特に，社会的責任にも配慮したコーポレートガバナンスと，それを支えるメカニズムである［ a ］の仕組みを，情報セキュリティの観点から，社内に構築・運用するよう指示があった。そこで，両課室は，次の検討を開始した。

・業務用 IT ツールの利用による営業効率の最大化及び営業活動の可視化
・情報セキュリティ対策の強化

両課室は，PC 管理ツール及びセキュア USB メモリ（以下，2 対策という）を旧 X 社のポリシの全社適用と同時に全社導入することを，2017 年 1 月中旬に全従業員に通知した。PC 管理ツールには，USB デバイス管理機能が含まれている。通知後，旧 Y 社の営業員から反対意見が管理課に寄せられたので，C 室長は旧 Y 社の情報資産の取扱いにおけるリスクを旧 Y 社の営業員に説明した。B 課長と C 室長は，旧 X 社のポリシの適用及び 2 対策の導入について，効果，業務への影響，現場の意見を確認するために，旧 Y 社の営業所 1 か所で試行導入することを検討した。B 課長と C 室長の検討の結果，反対意見が多く，情報資産の取扱いが最もずさんで，試行導入後の業務への影響が大きそうな北関東営業所で試行することを委員会に諮り，了承された。北関東営業所の概要を図 2 に示す。

・北関東3県の広域なエリアの顧客をカバーする営業所
・所長と事務補助員の他に，18名の営業員を配置
・通常，営業員は，日中，顧客先を回るために社有車を運転して外出
・合併以前の北関東営業所は，旧Y社の中でも業績の悪かった営業所の一つ
・旧X社南関東営業所の所長であったD氏が2016年10月に所長に任命され，業績を立て直し中

図2　北関東営業所の概要

〔メールの誤送信〕

北関東営業所での2対策の試行内容の概要は，図3のとおりである。2017年3月6日から，北関東営業所で旧X社のポリシの全面適用及び2対策の試行を開始した。

1. PC管理ツール
　(ア)　PC管理用サーバ
　　・業務PCの起動及び終了の履歴や利用者の操作履歴などを収集
　　・業務PCへの接続を許可するセキュアUSBメモリを登録
　(イ)　PC管理用クライアントソフト
　　・業務PCにインストールして利用し，業務PCの起動及び終了の履歴や利用者の操作履歴などをPC管理用サーバにアップロード
　　・PC管理用サーバに登録したセキュアUSBメモリだけ接続を許可
2. セキュアUSBメモリ
　・マルウェア対策ソフトを搭載し，ハードウェアによるデータ自動暗号化機能を実装
　・営業所内での貸与数は，試行における予算内で購入可能な10個
　・貸出しの制約条件：1人につき1個まで
　・利用したい者は，氏名，借用期間を記した借用申請書を所長に提出
　・シリアル番号をキーとした管理台帳に借用申請書上の利用者氏名及び借用期間を所長が記録

図3　北関東営業所での2対策の試行内容（概要）

2017年3月17日正午，北関東営業所の営業員のEさんの担当顧客M氏が，Eさんから，無題かつ本文なしであるが添付ファイル付きのメールを受信した。M氏は不審に思い，同日午後2時，その旨を営業所にいたD所長に電話で伝えた。その直後，D所長からM氏の電話内容を聞いたEさんは，誤送信をM氏に謝罪し，そのメールの削除を依頼した。そのメールには，社外秘文書ファイルが添付されていたが，そのファイルは旧X社のポリシに則して［　b　］してあった。そのため，M氏はファイルを開こうとしたが開くことができず，内容の確認ができなかったので，情報漏えいという重大な事故には至らなかった。D所長はこの件についてB課長に報告をした。B課長は，念のために，試行開始後，他の営業員もEさんと同様なメー

ル誤送信がないか D 所長に調査を依頼したところ，②メール誤送信には至らなかったが，送信直前の確認で宛先の間違いに気づいて修正してから送信した事例が 6 件あったという報告を受けた。B 課長は，このままでは後に重大な事故が起きると考え，メール誤送信未遂と E さんの件の詳しい調査を D 所長に依頼した。

〔情報セキュリティガバナンスの向上〕

D 所長は，E さんへの聞き取り調査の結果を，図 4 のとおり B 課長に報告した。

・2016 年度下期の営業成績が，目標未達であったので，業績改善に躍起になっていた。
・社外秘文書ファイルは，M 氏が所属する会社とは別の会社向けに，X 社からの値引き後の販売価格を提示するため，3 月 17 日午前中に，業務 PC で作り始めたものであった。その日は金曜日であったので，午後の客先訪問後，自宅に直帰し，土日に自宅で，③会社の許可を得ないまま，個人所有の PC を使用して社外秘文書ファイルの作成の続きを行うことにした。
客先訪問前に社外秘文書ファイルをセキュア USB メモリに入れて持ち出そうとしたが，全てのセキュア USB メモリが貸出し中であったので，E さんが使用できるものはなかった。
E さんの個人所有の USB メモリを業務 PC に接続したが，使用できなかった。
・旧 X 社のポリシには，メールクライアントソフトへの私用のメールアドレスの登録を禁止する条文がなかったので，E さんの私用のメールアドレスを登録したままであった。試行開始後も，社外秘文書ファイルを E さんの私用のメールアドレス宛てのメールに添付して送信し，自宅の個人所有の PC で編集を行っていた。
・社外秘文書ファイルは，1M バイトであったので，E さんの私用のメールアドレス宛てのメールに添付して送信を試みた。そのとき，メールクライアントソフトの宛先入力自動補完機能によって，先頭数文字が同じ M 氏のメールアドレスが誤選択された。午後の客先訪問に遅刻しそうで急いでいたので，宛先メールアドレスをよく確認せずに送信してしまった。

図 4　E さんへの聞き取り調査の結果

D 所長は，3 月 17 日時点でのセキュア USB メモリの管理台帳を確認し，貸出し中のものの中には，借用期限が過ぎたものが 5 個あったこと，1 人で 2 個以上のセキュア USB メモリを同時に借りていた営業員が 3 人いたことを B 課長に報告した。B 課長は，D 所長から報告を受けた直後，E さんが用いた業務 PC，メールアーカイブサーバなどの調査を経営企画室に依頼した。経営企画室が，④E さんからメールの添付ファイルのパスワードを聞きながら調査を進めたところ，試行開始後に E さんが旧 X 社のポリシに違反していたことが確認できた。そのため，B 課長は，E さんと話をしてメール誤送信の根本的な原因を明らかにすることにした。次は，そのときの B 課長と E さんの会話である。

B 課長：今回のメール誤送信の件は，情報漏えいには至りませんでした。M 氏がそのメール受信直後に当社に連絡してくれたので，我々もすぐに誤送信に気づくことができ，幸運でした。しかし，メール誤送信の根本的な原因を明らかにしたいと思っています。そもそも，なぜ，旧 X 社のポリシに違反して社外秘文書ファイルを送信したのですか。

E さん：試行のせいで業務の効率が悪くなったからです。

B 課長：業務の効率が悪くなったのは問題なので，解決していきましょう。ところで，試行内容について，詳しい説明はありませんでしたか。

E さん：いいえ，営業所内の営業員に対しては，試行開始直前，D 所長から試行の概要説明があっただけでした。

B 課長：なるほど。D 所長によるセキュア USB メモリの管理台帳の確認結果も，営業員への試行内容に関する説明が不十分だったことを示していますね。それで，図 4 のようなことになったのですね。

B 課長は，E さんとの会話の後，北関東営業所の営業員に試行内容を周知した。加えて，メールの宛先入力自動補完機能の使用禁止について意見を聴いた。そうしたところ，営業員から要望が出されたので，それらの要望を試行に関する報告書の一部として図 5 に取りまとめた。

(a) 業務 PC をノート型に変更し，社外での業務利用を可能にしてほしい。
(b) セキュア USB メモリの借用申請書の提出を廃止してほしい。
(c) セキュア USB メモリの営業所内での貸与数を，営業員数と同じにしてほしい。
(d) メールの宛先入力自動補完機能は便利なので，使用を継続させてほしい。
(e) 営業員の意見を取り入れる仕組みを設けてほしい。

図 5　B 課長が取りまとめた営業員からの要望

B 課長は，図 5 の各要望への対応とメール誤送信の防止をどのように両立させるかについて，C 室長に相談した。次は，C 室長と B 課長の会話である。

C 室長：(a) は，営業員の営業効率の向上には有効なので，同意します。ただし，(a) を実現するためには，⑤次の二つの条件を両方満たす対策が必要です。一

つ目はデータの漏えい・消失のリスク又はそれによる被害のリスクが低減可能であること，二つ目は社長方針に沿うことです。(b) 及び (c) については，D 所長によるセキュア USB メモリの管理台帳の確認結果と E さんへの聞き取り調査の結果から分かる問題のうち幾つかを解決すれば，(b) 及び (c) の要望自体が出なくなります。一方，(d) の宛先入力自動補完機能は，今回のメール誤送信を引き起こした原因の一つなので，無効化すべきと考えます。いかがですか。

B 課長：(b) 及び (c) については，C 室長の意見に賛成です。しかし，(d) については，この機能がないと，メールアドレスを全て手入力することになるので，非常に不便だと思います。旧 X 社のポリシに従った，かつ，誤送信も低減できる形で，メールの宛先の入力を便利にする方法はありませんか。

C 室長：二つの方法があります。一つ目は，宛先入力自動補完機能を無効化させた上で，［ c ］という方法です。二つ目は，宛先入力自動補完機能を無効化させずに，［ d ］という方法です。

B 課長：(d) は要望どおりとして，追加費用は掛かりますが，［ d ］という方法が，情報セキュリティ対策としてバランスが良いと思います。(e) については，現場の意見を聞くためのワーキンググループ（以下，現場 WG という）を立ち上げたいと思います。そして，現場 WG をまとめられる人材に現場 WG を運営してもらって，業務効率向上と情報セキュリティ対策強化が両立できる提案をまとめてもらえるよう，A 部長と相談します。

A 部長及び C 室長は，委員会において，試行結果及びメール誤送信の報告を行った。委員会では，始めは社長方針の実現のために［ e1 ］で取り組み，さらに現場の意見をくみ取るという［ e2 ］によってバランスを取るという B 課長の姿勢が高く評価された。A 部長は，B 課長からの相談内容について，現場 WG の設置を委員会に提案し，承認された。その後，4 月 1 日に旧 X 社のポリシが全社適用された。さらに，上場企業に必要な［ a ］の六つの基本的要素の一つである IT への対応の準備，全社的な業務の効率化，情報セキュリティガバナンスの強化が図られることになった。

設問1　〔情報システムの利用の変化〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，法改正に伴い，X社が個人情報取扱事業者に該当することになる理由として適切なものを，解答群の中から選べ。

解答群

ア　X社が，事業の承継に伴って旧Y社の顧客データの提供を受けたことが，個人データの第三者提供に該当するから

イ　改正後の政令の条文に個人情報取扱事業者から除かれる者の条件として，個人情報の数の条件が規定されており，X社が取り扱う個人情報の数が，その条件を満たさなくなるから

ウ　改正前の法に個人情報取扱事業者から除外される者の条件として，“その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者”という条文があったが，それが削除されたから

エ　非上場会社も個人情報取扱業者に該当することになったから

(2)　本文中の［　a　］に入れる適切な字句を，解答群の中から選べ。

aに関する解答群

ア　QCD

イ　資源ベースアプローチ

ウ　システムライフサイクルマネジメント

エ　内部統制

オ　不正検知

カ　プロジェクト統合マネジメント

設問2　〔メールの誤送信〕について，(1)，(2)に答えよ。

(1)　本文中の［　b　］に入れる適切な字句を，解答群の中から選べ。

bに関する解答群

ア　パスワードによって保護

イ　非可逆圧縮

ウ　ファイル変更履歴の記録を無効化

エ　ファイル変更履歴の記録を有効化

オ　ファイル名に“秘密”という文字を挿入

(2)　本文中の下線②について，このような事例を何というか。解答群の中から選べ。

解答群

ア　SPAMメール　　イ　内部不正

ウ　ヒヤリハット　　エ　標的型攻撃メール

オ　ポリシ違反　　カ　リスク受容

キ　リスク予防

設問3　〔情報セキュリティガバナンスの向上〕について，(1)～(5)に答えよ。

(1)　図4中の下線③のような行為はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　オープンイノベーション　　イ　シャドーIT

ウ　テレメタリング　　エ　テレワーク

オ　ノマドワーキング

(2) 本文中の下線④について，どのような調査方法でどのような違反が分かったか。次の (i) ～ (iv) のうち，調査方法と分かった違反が適切な組みだけを全て挙げた組合せを，解答群の中から選べ。

	調査方法	分かった違反
(i)	E さんが利用している業務 PC 上のメールクライアントソフトのメールアドレス帳を調査	E さんが，業務 PC 上のメールクライアントソフトのメールアドレス帳に自身の私用のメールアドレスを登録し，メールアドレス帳内で検索可能な状態にしていた。
(ii)	E さんが利用している業務メールアドレスについてメールアーカイブサーバを調査	E さんが，社外秘文書ファイルを添付したメールを自身の私用のメールアドレス宛てに送信していた。
(iii)	PC 管理ツールを用いて，E さんが利用している業務 PC の 3 月 17 日の操作履歴を調査	E さんが，会社の許可を受けていない個人所有の USB メモリに，業務 PC 内の社外秘文書ファイルをコピーし，それを個人所有の PC 上で編集していた。
(iv)	PC 管理ツールを用いて，E さんが利用している業務 PC の 3 月 17 日の操作履歴を調査	E さんが，業務 PC 上で作成した社外秘文書ファイルをセキュア USB メモリにコピーし，それを個人所有の PC 上で編集していた。

解答群

ア (i)　　イ (i), (ii)　　ウ (i), (iii)

エ (i), (iv)　　オ (ii)　　カ (ii), (iii)

キ (ii), (iv)　　ク (iii)　　ケ (iii), (iv)

コ (iv)

(3) 本文中の下線⑤について，次の (i) ～ (vii) のうち，対策として適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) BIOS のパスワードに，他人に推測されにくい文字列を設定

(ii) OS とアプリケーションのファイルを除く，ハードディスク中の全てのファイルに対し，ファイルごとに異なるパスワードを用いて手動で暗号化

(iii) OS のパスワードに，他人に推測されにくい文字列を設定

(iv) 機密性が高い情報を会社貸与のノート型の PC に格納することを原則として禁止し，営業成績を上げられる見込みがある場合に限り，営業員の判断でその情報をそのノート型の PC に格納可能とすることという条文を旧 X 社のポリシに追加

(v) 旧 X 社のポリシに則したパスワードを用いてハードディスク全体を暗号化

(vi) 社外で漏えい・消失が発生した場合の対応フローを策定

(vii) ディスプレイにのぞき見防止フィルタを装着

解答群

ア (i), (ii), (iii), (iv), (vi), (vii)

イ (i), (ii), (iv), (v), (vii)

ウ (i), (ii), (v), (vi), (vii)

エ (i), (iii), (iv), (v), (vi)

オ (i), (iii), (v), (vi), (vii)

カ (ii), (iii), (iv), (vi), (vii)

キ (ii), (iii), (v), (vi)

ク (ii), (iv), (v), (vi), (vii)

ケ (iii), (iv), (v), (vi), (vii)

コ (iii), (v), (vi), (vii)

(4) 本文中の［ c ］，［ d ］に入れる適切な字句を，解答群の中からそれぞれ選べ。

c，d に関する解答群

ア　顧客企業の購買担当者の一覧を顧客名簿ファイルとして，パスワードによる保護を施さずに保存しておき，そのファイルの中にあるメールアドレスをコピーして，メールクライアントソフトの宛先欄に貼り付ける

イ　電子署名方式の送信ドメイン認証技術を導入する

ウ　メールクライアントソフトのメールアドレス帳を活用し，メールを送信したい相手の氏名による検索によって，メールアドレスを選択する手順を従業員に教育する

エ　メール誤送信防止ツールを新たに導入してメール送信前に利用者が宛先を確認するための画面を表示し，即時送信を抑止する

オ　メールを送信したい相手から過去に受信したメールに対する返信としてメールを送信するとき，宛先がその相手だけであることを確認しない

(5) 本文中の［ e1 ］，［ e2 ］に入れる字句の適切な組合せを，e に関する解答群の中から選べ。

e に関する解答群

	e1	e2
ア	組合せアプローチ	ギャップアプローチ
イ	組合せアプローチ	ベースラインアプローチ
ウ	組合せアプローチ	リスクアプローチ
エ	トップダウンアプローチ	ベースラインアプローチ
オ	トップダウンアプローチ	ボトムアップアプローチ
カ	トップダウンアプローチ	リスクアプローチ
キ	ホールシステムアプローチ	ギャップアプローチ
ク	ホールシステムアプローチ	組合せアプローチ
ケ	ホールシステムアプローチ	ボトムアップアプローチ

〔 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	13:10 ～ 13:50

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。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，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。