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