問1　情報セキュリティインシデント対応状況の監査に関する次の記述を読んで，設問1～4に答えよ。

B社は，中規模のインターネットサービス企業であり，買収した国内の子会社2社を含めて，B社グループとして事業を展開している。

〔B社グループの情報セキュリティインシデント対応体制〕

B社グループは昨年4月，情報セキュリティインシデント（以下，インシデントという）への対応体制強化のために，B社CSIRT（Computer Security Incident Response Team）を設置した。B社グループにおけるB社CSIRTの位置付け，及び国内外の外部CSIRTなどの外部関連組織・外部Webサイトとの関係を，図1に示す。

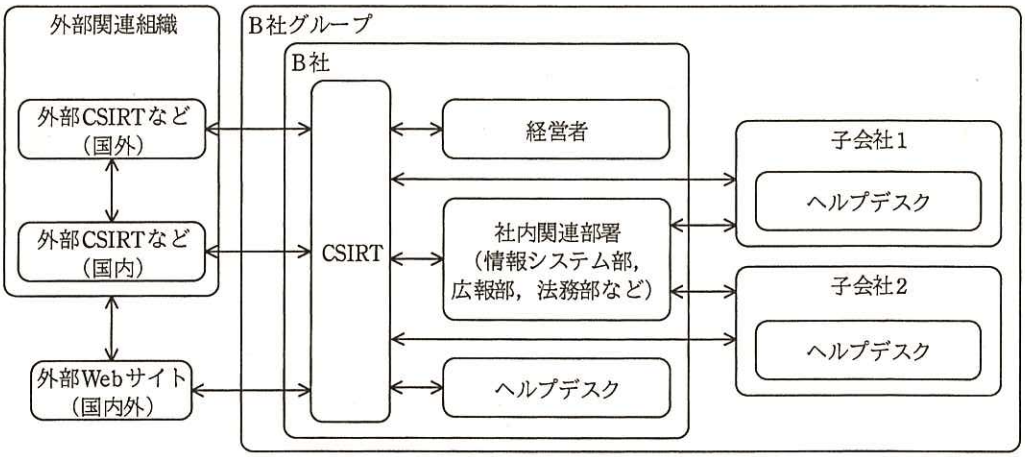

図1　B社CSIRTの位置付け及び外部関連組織・外部Webサイトとの関係

B社CSIRTは，B社の役員及び従業員で構成され，メンバは，最高責任者であるCIO，情報セキュリティに精通した専任社員（以下，専任社員という）2名，情報システム部との兼任社員（以下，情シ兼任社員という）2名，及びインシデント対応関連部署（広報部，法務部など）との兼任社員5名である。これらの兼任社員7名は，各子会社の対応する同部署との連絡窓口にもなっている。

B社CSIRTの対応範囲は，基本的にB社グループ内であるが，必要に応じて外部関連組織と連携して対応する場合がある。

〔インシデント対応状況の監査〕

年度監査計画に基づき，B 社内部監査部のシステム監査人 2 名が，設置後 1 年を経た B 社 CSIRT におけるインシデント対応状況の監査を行った。

監査の結果，判明した事項は，次のとおりである。

(1) B 社グループが共通で利用している電子メールシステム及びイントラネットを除き，B 社グループ各社の情報基盤は，IDS などの検知システムを含め，それぞれの情報システム部門が独自に管理している。検知システムは，B 社 CSIRT 設置以前に，B 社グループ各社が導入していたものである。

(2) B 社 CSIRT の最も重要な役割は，情報セキュリティイベント（以下，イベントという）の認知・連絡受付から通知・報告などに至る一連の活動（以下，インシデントハンドリングという）である。その内容を，表 1 に示す。

表 1 B 社 CSIRT が行うインシデントハンドリングの内容（抜粋）

項番	項目	内容
1	イベント認知・連絡受付	(1) 検知システムによって検知され，インシデントと自動判定されたイベントの認知 (2) B 社グループ内のヘルプデスク経由の連絡又は DNS などのディレクトリサービスを利用した外部連絡によるイベントの受付
2	トリアージ	(1) 認知又は連絡受付済みのイベントについて，B 社 CSIRT が対応すべきかどうかの判断及び必要に応じて行う連絡元への回答 (2) B 社 CSIRT が対応すべきイベントについて，インシデント判定マニュアルに基づく，インシデントかどうかの最終判定及び対応の優先順位付け
3	インシデントレスポンス	(1) B 社グループ内で発生したインシデントについて，当該会社のシステム管理者などとの連携及び被害の極小化・拡大防止を図るための対応 (2) 当該インシデントの影響が外部 Web サイトに及ぶおそれがある場合の，外部関連組織との情報交換及び必要な対応
4	B 社グループ内への通知・監督官庁への報告など	(1) B 社グループ内での被害の極小化・拡大防止を図るための注意喚起 (2) 必要に応じて行う監督官庁への報告，メディアや一般向けの公表など，外部への対応

(3) B 社 CSIRT は，イベントを“B 社グループの情報セキュリティに影響を及ぼし，重大な情報セキュリティ事故につながるおそれがある事象”と定義している。さらに，イベントの中でも“重大な情報セキュリティ事故に至り，B 社グループに多大な被害を与える事象”をインシデントと定義し，インシデントレスポンスの対象としている。

(4) B 社グループ各社の検知システムで検知されたイベントは，インシデントかどうか自動判定が行われ，インシデントと判定された場合には，B 社 CSIRT にも自動的に通知される。

このときに使用される，イベントの検知基準及びインシデントの自動判定基準は，検知システム上で設定されており，これらは，B 社 CSIRT 設置時に一度見直しが行われている。しかし，それ以降は検知システム上の設定が見直されておらず，検知システムで問題が発生するおそれがある。

(5) 専任社員及び情シ兼任社員は，B 社 CSIRT に常駐している。情シ兼任社員は，インシデントハンドリングにおいて，トリアージを含め，専任社員の職務を担当することもある。トリアージで使用するインシデント判定マニュアルには，判定のための確認事項及び確認方法が記述されている。このマニュアルは，トリアージについて高いスキルをもつ技術者向けに策定されているので，全ての確認事項について，詳細な確認方法が記述されているわけではない。

また，情シ兼任社員 2 名は，専任社員と同等のスキルをもっておらず，トリアージを常に正確に行うのは困難と判断される。このため，確認事項によっては，トリアージが適切に行われないおそれがある。

(6) 最近，B 社 CSIRT が，子会社の一つでインシデントレスポンスを行ったとき，一部のネットワーク機器が生成するログレコードの形式が，当該機器のバージョンアップで変更されており，そのまま使用することができなかった。その影響で，被害範囲の特定及び対応策の検討に時間を要し，結果的にインシデントハンドリングの完了が遅れた。

現在の運用のままでは，インシデントが発生した場合，再度インシデントハンドリングに支障を来すおそれがある。

(7) B 社 CSIRT 設置の際に外部関連組織との連携体制を構築して以降，定期的な情報交換や外部関連組織リストの更新などを行っていない。外部関連組織との連携体制の維持・強化は，B 社 CSIRT 運用規程で定められているが，日々発生するイベントの認知・連絡受付やトリアージに追われ，後回しになっている。

その結果，B 社グループ内又は外部でインシデントが発生した場合，外部関連組織との連携が迅速かつ有効に行われないおそれがある。

設問1　〔インシデント対応状況の監査〕の(4)について，システム監査人は，どのような問題が発生するおそれがあると考えたか。問題を一つ挙げ，35 字以内で述べよ。

設問2　〔インシデント対応状況の監査〕の(5)について，システム監査人は，どのような監査手続を実施した結果，“情シ兼任社員 2 名は，専任社員と同等のスキルをもっておらず，トリアージを常に正確に行うのは困難”と判断したか，45 字以内で述べよ。

設問3　〔インシデント対応状況の監査〕の(6)について，システム監査人は，B 社 CSIRT が，B 社グループ各社と連携してどのような対策を実施すべきと考えたか，40 字以内で述べよ。

設問4　〔インシデント対応状況の監査〕の(7)について，システム監査人が想定した，“外部関連組織との連携が迅速かつ有効に行われない”ことによる影響を，次の(1)及び(2)の観点から，それぞれ 50 字以内で述べよ。

(1)　B 社グループ内に及ぼす影響

(2)　B 社グループ外に及ぼす影響