問3　制御ネットワーク及び制御システムの監査に関する次の記述を読んで，設問 1～4 に答えよ。

D 社は，エネルギー企業グループ系列の中規模の石油精製会社である。東京に本社があり，東日本で製油所を操業している。

〔D 社ネットワークの統合〕

D 社では，老朽化した製油所の装置設備を，10 年前に改装した。その際，製油所の石油精製制御システム（以下，制御システムという）も刷新した。また同時に，制御システムが接続されている製油所のネットワーク（以下，制御ネットワークという）と，生産管理システムなどの各種業務システム（以下，業務システムという）が接続されているネットワーク（以下，本社基幹ネットワークという）を統合した。

D 社の現在のネットワーク構成（概要）を，図 1 に示す。

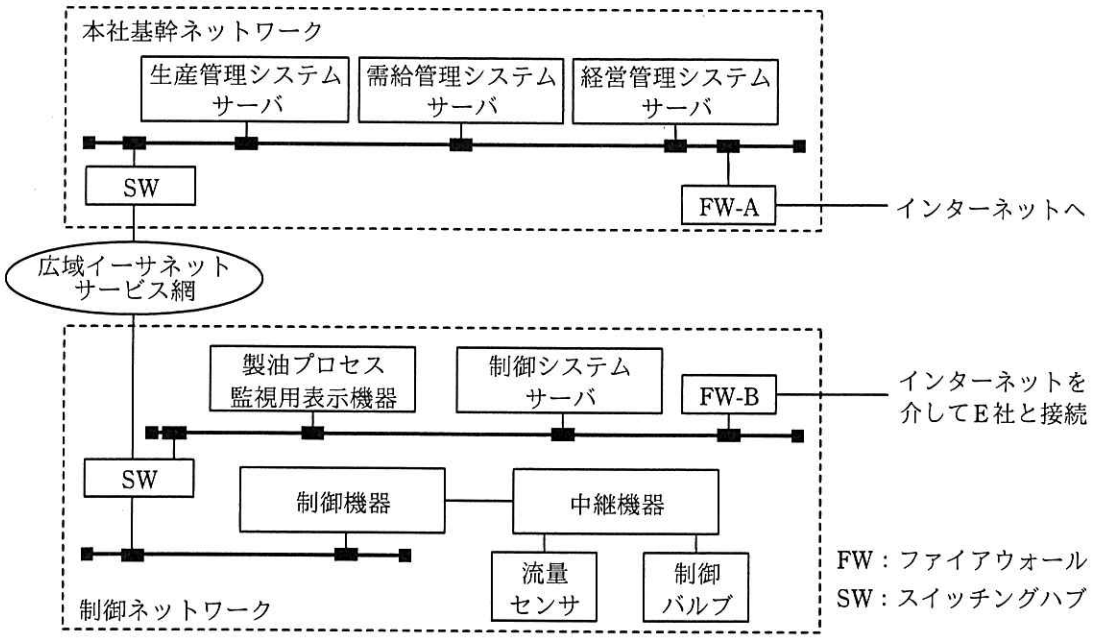

図 1　D 社のネットワーク構成（概要）

制御ネットワークは，広域イーサネットサービス網で本社基幹ネットワークと接続されている。また，制御システムの遠隔監視・保守のために，インターネットを

介して，制御システムの導入を担当したベンダであるE社と接続されている。

〔制御システムの刷新及び業務システムとの連携〕

刷新前の制御システムは，E社独自のシステム機器及び通信プロトコルを使用して構築され，製油所内の閉域ネットワークで稼働していた。その後の情報技術の進歩で，一部の装置を除き，汎用のシステム機器を用いることが可能になったので，刷新時に，コスト面で優位であるそれらの機器を導入した。また，汎用の通信プロトコルを利用して，制御システムを業務システムの一つである生産管理システムと連携させ，リアルタイムにデータを共有することによって生産性の向上を図った。その後，順次，需給管理システム及び経営管理システムとも連携させ，D社の経営効率の向上を図ってきた。

〔予備調査の実施〕

最近，他社で制御ネットワーク及び制御システムの脆弱(ぜいじゃく)性を突いたセキュリティインシデントが発生したことを受け，D社の社長は，内部監査部長に制御ネットワーク及び制御システムのセキュリティ管理状況を監査するよう指示した。

制御ネットワークは本社基幹ネットワークと接続されていることから，システム監査人は，予備調査の一環として，それぞれのネットワーク及びシステムのセキュリティ管理の相違点について比較し，表1のとおりまとめた。

表1　セキュリティ管理の相違点（抜粋）

項番	比較項目	制御ネットワーク 及び制御システム	本社基幹ネットワーク 及び業務システム
1	セキュリティ管理規程	製油所安全管理規程	情報セキュリティ管理規程
2	セキュリティ管理部署	製油所の操油部計装課	本社の情報システム部セキュリティ管理課
3	セキュリティ管理者	機械及び電気の専門技術者	情報セキュリティの専門技術者
4	セキュリティ管理の考え方	物理的セキュリティを重視	物理的セキュリティに偏らない，バランスがとれたセキュリティを重視
5	優先されるセキュリティ要件	24時間365日連続稼働（装置設備の法定点検時などの停止を除く）	情報漏えいからのデータ保護

〔本調査での発見事項〕

システム監査人による本調査の結果，次のことが判明した。

(1) 表 1 の項番 1～3 について，製油所安全管理規程及び情報セキュリティ管理規程の改訂は，ネットワーク統合時に各セキュリティ管理部署主管で行われている。また，製油所安全管理規程の承認は製油所安全管理委員会で，情報セキュリティ管理規程の承認は情報セキュリティ管理委員会で，それぞれ行われている。

これらの規程では，ネットワーク及びシステムのセキュリティ管理において遵守すべきルール，セキュリティ管理部署及びセキュリティ管理者の役割と責任範囲などが定められている。しかし，両規程は個別に策定されており，D 社における全社的なセキュリティ管理の観点からは内容の確認が行われていない。

(2) 表 1 の項番 4 について，制御ネットワークでは，物理的セキュリティが重視されており，本社基幹ネットワークに比べてセキュリティ管理対象が限定されている。

したがって，マルウェアの物理的な感染経路である USB ポートは，セキュリティ対策が講じられているが，制御ネットワークへの論理的アクセス制御やサーバのハードニングなど，管理対象として重視されていないセキュリティ領域の対策が不十分である。このため，システム設定上の不備に起因するセキュリティインシデントが発生するおそれがある。

(3) OS 開発元が提供するセキュリティパッチを制御システムに適用するに当たっては，表 1 の項番 5 に示したセキュリティ要件を満たすことを，セキュリティ管理者が事前に確認する必要がある。さらに，制御システムは，製油プロセスを制御データの数値によって正確にタイミングよく制御するために，プログラムロジック及びパラメタ値が最適化されている。このため，制御データ処理時の数値の変動とタイミングの変化が定められた範囲に収まることも，セキュリティ管理者が事前に確認する必要がある。

また，セキュリティパッチ適用の間隔が比較的長いこともあり，その間の OS の脆弱性を突いたセキュリティインシデント発生に備えた補完的コントロールが必要である。

(4) 操油部計装課には情報セキュリティの専門技術者がいないので，図 1 に示した FW-B の設定は，E 社が推奨するポリシに基づいて，E 社の技術員が行っている。

また，操油部計装課は，FW-B 経由の遠隔監視・保守に伴う不正アクセスを防ぐために，次の対策①，②を講じるよう E 社に求めている。さらに，各対策が適切に行われていることを確認するために，四半期ごとに E 社から報告を受けている。

対策① 遠隔監視・保守を行うために制御ネットワークに接続する端末及びその利用者を限定する。

対策② 制御ネットワークへのアクセス状況を記録し，遠隔監視・保守以外の操作の有無を，製油所安全管理規程で定められた頻度で確認する。異常が発見された場合には，直ちに操油部計装課に報告する。

設問１ 〔本調査での発見事項〕の(1)について，“D 社における全社的なセキュリティ管理の観点からは内容の確認が行われていない”ことから，システム監査人が，製油所安全管理規程と情報セキュリティ管理規程に関して確認すべき内容を，40 字以内で述べよ。

設問２ 〔本調査での発見事項〕の(2)について，システム監査人が想定した“システム設定上の不備に起因するセキュリティインシデント”とは何か。50 字以内で述べよ。

設問３ 〔本調査での発見事項〕の(3)について，次の(1)，(2)に答えよ。

(1) セキュリティ管理者によるセキュリティパッチ適用前の確認が行われていることを，システム監査人が確かめる場合，どのような文書を査閲すべきか。二つ挙げ，それぞれ 20 字以内で答えよ。

(2) システム監査人が想定した“OS の脆弱性を突いたセキュリティインシデント発生に備えた補完的コントロール”を，20 字以内で答えよ。

設問４ 〔本調査での発見事項〕の(4)について，システム監査人が，対策①，②の他に，制御ネットワーク側で遠隔監視・保守に伴う不正なアクセスを防ぐための技術的対策が適切に講じられていることを確認するための監査手続を，50 字以内で述べよ。