問9　セキュリティインシデントへの対応に関する次の記述を読んで，設問1～4に答えよ。

E社では，外部から自社ネットワークへの不正アクセスなどの脅威に備えて，社内LANとインターネットとの接続ポイントにファイアウォールを設置している。それに加えて，よりセキュリティ強度を高めるために，ネットワーク型侵入検知システム（以下，IDSという）を図1のように設置した。

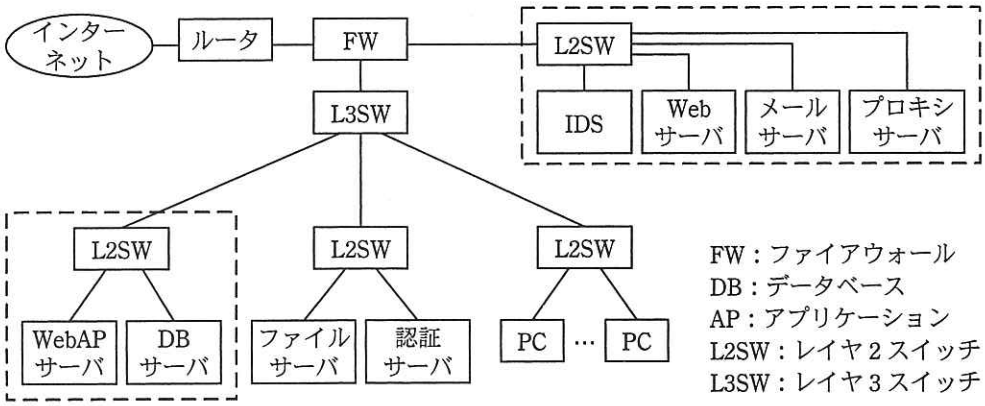

図1　ネットワーク構成

〔インシデントの発生〕

IDSの稼働開始の翌日，情報システム部セキュリティ担当のF主任が業務終了後に帰宅しようとしたところ，IDSからのアラートに気付いた。すぐに，上司であるG課長に連絡し，対応を開始した。しかし，情報システム部では，インシデント発生時に，どのような関係部署や社外の関係機関に連絡すればよいかを文書化しておらず，連絡に漏れと遅れが生じた。

アラートへの対応はG課長とF主任が中心になって実施し，対応に必要な要員を確保するのに時間を要したが，結果的に大きな問題は生じなかった。今回の事態を重視した情報システム部のH部長は，インシデント発生から対応完了までの手順に問題がなかったかを検証するために，F主任が作成したインシデント報告書を精査するとともに，G課長やF主任など，当日対応に当たった関係者から詳しい状況を聴取した。

〔インシデント対応の整理〕

関係者から聴取した内容に基づいて，H 部長は，今回のインシデントへの対応を，次の(1)～(8)のように整理した。

(1) アラートの内容から，インターネット上の特定のサイトから自社の Web サーバに対する ping の発生頻度が高く，外部からの攻撃の疑いがあると判断した。その判断に基づいて，G 課長と F 主任が相談の上で，初動対応を次のように実施した。

まず，危機管理担当部署など，インシデントの発生を認識する必要のある自社の関連部署に連絡した。次に，対応手順を検討し，“発生した事実の確認”，“影響の内容と範囲の調査”，“インシデントの原因と発生要因の特定”，“対策の検討と実施”の順で行うことにした。

(2) 続いて，G 課長は，アラートの内容から対応に必要となる要員を選定し，情報システム部のオペレーション室に参集するよう連絡を取ろうとした。しかし，全ての情報システムの機能やネットワーク構成，及びシステム間での機能やデータの連携関係が詳細に把握できていなかったので，要員選定に非常に手間取った。

(3) 必要な要員の参集後，G 課長の指示の下で各要員が手分けして，次の(4)～(8)の作業を進めた。

(4) アラートの発生状況や意味について事実を確認し，情報を整理した。また，インシデント発生時の状況を示す記録として，各サーバへのログイン状況，外部とのネットワーク通信状況，各サーバのプロセスの稼働状況に関する［ a ］をコピーした。

(5) 通常業務が終了した時間帯であったので，特段の連絡は行わずに，発生したインシデントとの関連が懸念されるネットワークセグメント（図 1 で，破線で囲った二つのセグメント）を，外部ネットワーク及び社内 LAN の他のセグメントから切断した。この点に関しては，残業をしていた部署から情報システム部の担当者にクレームがあった。

(6) インシデントによってもたらされた影響の有無とその内容・範囲を明確にするために，アラートに関連するログを調査し解析した。具体的には，サーバのシステムログからサーバへのログインやサーバ内のファイルへのアクセス状況を調査した。また，インシデントが検知されたネットワーク内の各サーバから外部に異常な通信がないかどうか，ファイアウォールと IDS のログを調査した。調査に当たっては，

ログが［ b ］されたおそれがないかを事前に検証した。ログの解析作業において，各ログ間の前後関係がすぐには特定できず，作業に手間取った。

(7) ログの調査結果と各種設定値の確認結果に基づき，インシデントの原因と発生要因の特定を進めた。その際，IDS ではアノマリー検知における［ c ］があり得ることを念頭においた。特定作業の結果，アラートが発せられた原因は，E 社の取引先が E 社の Web サーバとの通信における応答時間を ping コマンドを使って測定する際に，ping コマンドのオプション項目を誤って指定したことによって，ping が短時間に大量に発信されたことであったと判明した。

(8) インシデントの原因調査と並行して，社外の関係機関への連絡を準備するよう要員に指示したが，インターネット上の他サイトは連絡の対象外とした。これは，E 社のサーバが［ d ］に利用されたおそれが低いと判断したからである。

その後，インシデントの発生要因への対策，システムの復旧，再発防止策を実施した。

〔H 部長の意見〕

インシデント対応の経緯を整理した H 部長は，G 課長に次のような指摘をして，対応手順を見直すよう指示した。

(1) インシデント発生時の連絡体制の整備について

・今回関係者への連絡が遅れたという事実への反省から，インシデント発生時に連絡すべき社内各部署の責任者，及び外部の機関を一覧にして連絡先を記載し，それを関係者に配布する。

・インシデントの内容や発生場所に応じて，［ e ］し，連絡先とともに文書化する。

(2) 対応手順の整理について

・一部の部署には影響があったが，対応手順に大きな問題はなかった。しかし，対応手順をその場で検討するのではなく，インシデントの内容や発生場所ごとに手順をあらかじめ想定して，それを文書化しておくべきである。

・〔インシデント対応の整理〕の(5)については，今回の対応ではやむを得なかったが，セキュリティに関する攻撃を受けたおそれがあるなどの限定された状況以外では，ネットワークの切断を実施すべきではない。まず，対応手順の実施によっ

てインシデントの影響範囲を拡大させないこととともに，インシデントの原因・影響の調査に必要となる記録を消滅させないことや業務へ影響を及ぼさないという，二次的損害の防止を考慮して対応手順を実施すべきである。また，実施に当たっては，［ f ］を怠らないことも重要である。あわせて，意思決定プロセスや判断基準をあらかじめ制定しておくことも検討すべきである。

・今回の対応では，〔インシデント対応の整理〕の(6)のログの解析作業において，各ログ間の前後関係がすぐには特定できず，作業に手間取るという事象が発生した。①このための対策を実施すべきである。

設問1　本文中の［ a ］～［ d ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　SQLインジェクション攻撃　　イ　改ざん

ウ　誤検知　　エ　シグネチャ

オ　盗聴　　カ　踏み台

キ　マッチング　　ク　ログ

設問2　本文中の［ e ］に入れる適切な字句を20字以内で答えよ。

設問3　本文中の［ f ］に入れる適切な字句を，〔インシデント対応の整理〕(5)で示された問題点を参考にして，30字以内で答えよ。

設問4　本文中の下線①について，最も適切な対策を解答群の中から選び，記号で答えよ。

解答群

ア　NTPサーバをネットワーク内に設置して，各機器の時刻を同期させる。

イ　SNMPを使って，機器の情報を収集する。

ウ　ログ解析ツールを導入する。

エ　ログのバックアップを，書換え不能な媒体に取得する。