問2　ソフトウェアの脆弱性への対応に関する次の記述を読んで，設問1～3に答えよ。

B社は，従業員数400名で昨年度の年間売上高が80億円の菓子製造業者であり，インターネット上のWeb販売システムにおいて自社製品の販売を行っている。このWeb販売システムの管理は社内のシステム運用部が行っている。Web販売システムの構成を図1に，Web販売システムの概略仕様を図2に示す。

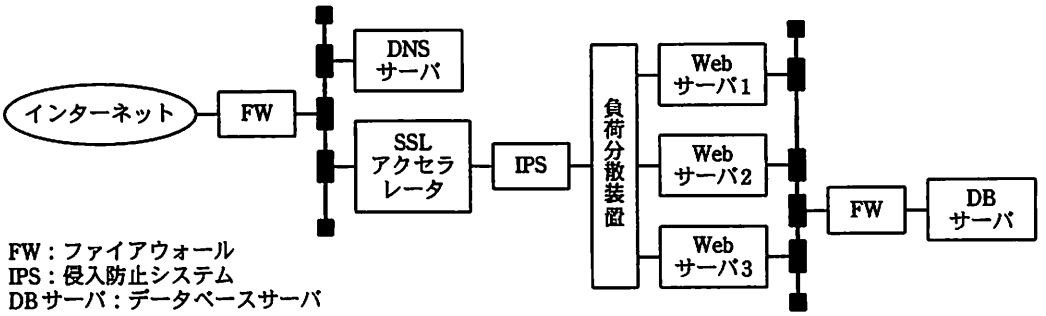

図1　B社のWeb販売システムの構成

(a) Webサーバ上では，主にHTTP送受信を処理するWebサーバプログラムと，主にDBサーバと連携して動的コンテンツ生成を行うWebアプリケーションが稼働している。
(b) Webサーバプログラムと Webアプリケーションは，限定された権限でも動作可能である。
(c) SSL暗号化，復号処理はSSLアクセラレータで行っている。
(d) いずれのFWも，アプリケーション層を解釈する機能はもっていない。
(e) DBサーバには，顧客の個人情報（住所，氏名，電話番号など機密性の高い情報）が格納されており，Webサーバ上のWebアプリケーションから参照，更新される。
(f) Webサーバプログラムは，システム管理者権限で動作している。
(g) Web販売システムの開発のために，B社のシステム開発部で図1とほぼ同一構成である動作試験用システムを別に用意している。

図2　B社のWeb販売システムの概略仕様（抜粋）

〔脆弱性情報の発見〕

B社は情報セキュリティ専門会社からセキュリティ情報の提供を受けている。ある日，Web販売システムで使用中のWebサーバプログラムに脆弱性が発見されたとの情報が提供された。このWebサーバプログラムの脆弱性情報を図3に示す。

・HTTP POST メソッドにおいて，HTTP ヘッダ内に RFC で定義されていない“X-Sender”というヘッダフィールドを指定することで，任意の OS コマンドを実行させることが可能である。その際，OS コマンドは Web サーバプログラムの動作権限で実行される。
・そのほかのメソッドでは，この脆弱性は報告されていない。
・Exploit コードが公開されている。

図 3　Web サーバプログラムの脆弱性情報（抜粋）

〔脆弱性の評価〕

次は，Web サーバプログラムの脆弱性に関する，システム運用部の P 君と Q 課長との会話である。

P 君　：当社が Web 販売システムで使用している Web サーバプログラムに脆弱性が存在することが報告されました。

Q 課長：まず対処の緊急性を検討しよう。図 4 に示す当社の脆弱性評価規程に当てはめると判定結果はどうなるのか。

P 君　：私は損害金額の算出が難しい場合の基準を適用し，<u>①“緊急”に相当すると判定しました</u>。

・ソフトウェアの脆弱性評価は，対処の緊急性の観点から，緊急，重要，注意の 3 段階判定とし，次の表に示す定義に基づき判定する。

表　脆弱性評価基準表

評価	脆弱性によって引き起こされることが想定される被害	
	損害金額が算出可能な場合 (*1)	損害金額の算出が難しい場合 (*2)
緊急	被害によって年間売上高の 1%に相当する金額を超える経済的損害が発生する。	次の事象によって顧客からの信頼を大きく損なう。 (1) 機密性の高い情報が漏えいする。 (2) システムの機能が全面的に停止する。
重要	被害によって年間売上高の 1%に相当する金額以下の経済的損害が発生する。	次の事象によって顧客からの信頼を損なう。 (1) 機密性の低い情報が漏えいする。 (2) システム性能が部分的に低下する。 (3) ログの内容が漏えいする。
注意	経済的損害は発生しない。	顧客からの信頼を損なうおそれは少ない。 例)・システム設定ファイルの内容が漏えいする。 ・CGI スクリプトファイルのソースコードが漏えいする（ほかの被害にはつながらない）。

注 損害金額が算出可能な場合は (*1) を使用し，算出が難しい場合は (*2) を使用して判定する。
損害金額の算出には，間接的損害は算入しない。

図 4　B 社の脆弱性評価規程（抜粋）

Q課長：私も“緊急”と判定する。それに，②図 3 の脆弱性情報から考えても，攻撃が実際に行われる可能性が高い。早速，対策の検討を開始しよう。運用管理グループリーダのS君を呼んでくれ。

〔暫定的対策の検討〕

Q課長：それでは今回の脆弱性について対策の検討を始めよう。P 君，考えられる対策には何があるのか。

P君　：現在，開発元から Web サーバプログラムの修正プログラムが提供されていないので暫定的対策となりますが，POST メソッドでのアクセスを拒否する方法が考えられます。

S君　：Web 販売システムで POST メソッドでのアクセスを拒否すると，HTML 文書の［　a　］要素内に利用者が入力したデータを受け付けることができず，製品の販売ができなくなってしまいます。HTML 文書を修正して，POST メソッドを GET メソッドに置き換えた上で POST メソッドでのアクセスを拒否するという対策であれば，製品販売も続けられます。

Q課長：いや，GET メソッドを使用するとクエリストリングに利用者が入力した情報が含まれることとなり，POST メソッドと比較して③新たな情報漏えいの可能性が生じる。その方法ではなく，Web 販売システムに設置してある IPS に暫定的対策として拒否条件を追加することはできないのか。

P君　：この IPS では，④シグネチャをカスタマイズすることで実現可能だと思われます。

S君　：IPS による対策であれば，システム運用上大きな問題はないと思われます。

Q課長：それでは，IPS による暫定的対策を実施することとする。P 君は IPS のカスタマイズの準備にかかってくれ。また，修正プログラムの適用が完了するまで，Web アクセスログ，IPS の検出ログの確認頻度を 1 日 3 回に増やして，Web 販売システムに関する監視を強化することとする。

この検討の後，速やかに IPS による暫定的対策を実施した。

〔修正プログラムの適用〕

暫定的対策を実施した日から 10 日後に，P 君は，脆弱性に対応する修正プログラムの提供が開始されたことを Q 課長に報告した。報告には S 君も同席した。

P 君　：Web サーバプログラムの脆弱性に対応する修正プログラムの提供が開始されました。早急に，Web サーバに適用したいと思います。

Q 課長：今回の脆弱性と対策について営業課の T 課長に説明したところ，“1 週間前に当社の製品がテレビ番組で取り上げられた。その直後から，Web 販売システムでの販売が著しく伸びているので，システムを停止されては困る。”との意見が返ってきた。この意見も尊重した上で適用時期と適用方法について検討してほしい。

P 君　：しかし，暫定的対策は完全なものとはいえず，速やかに修正プログラムを適用すべきだと考えます。例えば，夜間など一時的に負荷が軽くなる時間帯を選んで適用作業をしてはいかがでしょうか。

S 君　：過去 1 週間の傾向では，昼間の時間帯はサーバ 3 台の処理能力がフルに必要なほどアクセスが多いのですが，深夜 2 時から朝 8 時までの間はアクセスが少なく，サーバ 1 台でも処理が可能な状態となっています。

P 君　：修正プログラムの適用に必要な作業時間は，サーバ 1 台当たり何時間と想定されるのでしょうか。

S 君　：サーバの停止から修正プログラムの適用，再起動まで含めておおよそ 30 分程度で完了すると見込まれます。

P 君　：それでは，図 5 に示す手順で作業を行えば，Web 販売システムを停止させることなく修正プログラムを適用することができるのではないでしょうか。

次の(1)～(3)の手順を，Web サーバ 1～3 の全 3 台に対して順次適用する。
(1) 対象となる Web サーバを [b] ために，負荷分散装置の設定を変更する。
(2) 対象となる Web サーバの Web サーバプログラムに修正プログラムを適用する。
(3) 負荷分散装置の設定を元に戻す。

図 5　修正プログラム適用手順案

Q課長：確かに，この手順であれば修正プログラムの適用が可能だ。⑤T 課長に修正プログラム適用手順，実施日時を説明した上で速やかに修正プログラムの適用を実施しよう。

その後，T 課長への説明も済み，図 5 の手順によって速やかに修正プログラムの適用を実施することになった。その結果，Web 販売システムの停止を伴うことなく脆弱性の対策が完了した。

設問 1　〔脆弱性の評価〕について，(1)，(2) に答えよ。

(1) 本文中の下線①において，P 君が脆弱性について“緊急”に相当すると判定した具体的根拠は何か。50 字以内で述べよ。

(2) 本文中の下線②において，Q 課長が，攻撃が実際に行われる可能性が高いと考えた根拠は何か。25 字以内で述べよ。

設問 2　〔暫定的対策の検討〕について，(1) ～ (4) に答えよ。

(1) 本文中の［ a ］に入れる適切な HTML の要素名を，英文字 6 字以内で答えよ。

(2) 本文中の下線③について，情報漏えいの可能性が生じる理由を，“クエリストリング”という語を用いて 70 字以内で述べよ。

(3) 本文中の下線④について，暫定的対策を実現するために拒否条件として IPS に登録すべきシグネチャの具体的内容を，40 字以内で述べよ。

(4) 本文で述べている IPS による対策に加えて，図 2 中の仕様の一部の設定を変更する対策も可能である。この一部とは図 2 中の (a) ～ (g) のいずれであるかを記号で答えよ。また，対策の内容について 30 字以内で述べよ。

設問 3　〔修正プログラムの適用〕について，(1)，(2) に答えよ。

(1) 図 5 中の［ b ］に入れる適切な字句を，15 字以内で述べよ。

(2) 本文中の下線⑤について，Web 販売システムにおける修正プログラム適用後のトラブルを予防するために，T 課長への説明の前に実施すべき作業がある。適切と思われる作業内容を，40 字以内で述べよ。