問3　ネットワークのセキュリティ対策に関する次の記述を読んで，設問 1～4 に答えよ。

X 銀行は，Q 県を本拠地とする中堅の地域金融機関である。X 銀行は，基幹システムである勘定系システムの運用を他行との共同センタに委託しているが，自行にもコンピュータセンタをもっており，インターネットバンキングは X 銀行独自のシステム（以下，IB システムという）で運用している。IB システムの構成を，図 1 に示す。

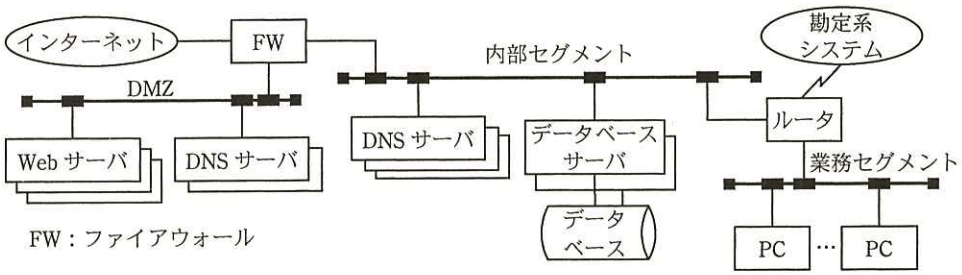


図 1　IB システムの構成（抜粋）

IB システムは，Web を使ったインターネット経由の顧客向けサービスである。IB システムは，勘定系システムで管理している口座残高などの情報を除き，独自のユーザ ID，パスワードなどの重要情報をデータベースに保有している。IB システムの Web サーバは，業務セグメントの PC からもアクセスできる。

最近，IB システムへのサイバー攻撃が増加している。金銭的な被害は発生していないが，セキュリティインシデントは頻繁に発見されている。

〔サイバー攻撃対策〕

X 銀行では，サイバー攻撃対策のためのセキュリティ担当者として，システム企画部の主任の F 氏が任命されている。次は，新たにシステム企画部に着任した G 君と，F 氏の会話である。

G 君：最近のサイバー攻撃にはどのようなものがあるのですか。

F 氏：最近，標的システムへの通信量を増大させて，ネットワークやサーバの処理能力を占有することによって，正常な取引の処理を妨害し，場合によってはサーバをダウンさせる DoS 攻撃が，頻繁に発生している。特に，多数のコンピュー

タが標的サーバを集中的に攻撃する［　ア　］型 DoS 攻撃は，発信元のコンピュータの特定が難しいので，被害が大きくなるといわれている。DoS 攻撃には，TCP のパケットを大量に送信し，応答待ちにして新たな接続を妨害する SYN［　イ　］攻撃や，コネクションレスの UDP パケットを使った UDP［　イ　］攻撃などがある。

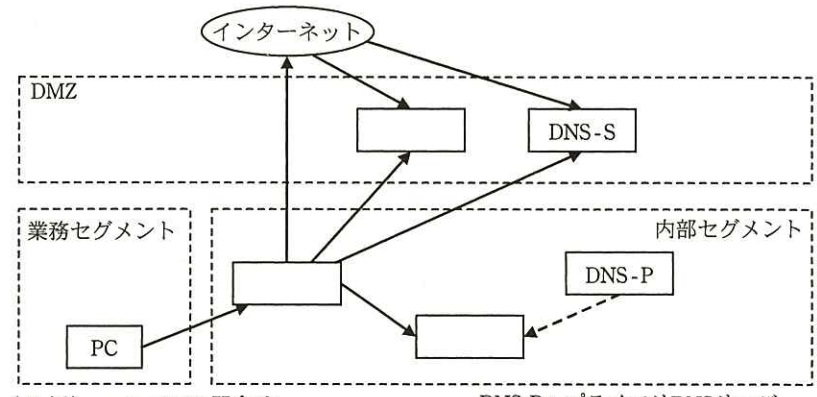
G 君：DoS 攻撃といえば，DNS の機能を悪用したものがあるそうですね。

F 氏：例えば，PC などから問合せを受けた DNS サーバが，他の DNS サーバにも問合せを行い，最終的な結果を返信する［　ウ　］的な問合せにおいて，発信元の IP アドレスを詐称して，その問合せの結果を標的サーバ宛てに送信させる DNS［　エ　］攻撃と呼ばれるものがある。このような，オープンリゾルバを用いた攻撃に関しては，自らも攻撃の［　a　］とならないようにすることが重要だ。サイバー攻撃に対応するためには，常に最新のセキュリティ対策を施しておく必要がある。

X 銀行では，DNS へのサイバー攻撃に対応するために，IB システムに様々な対策を施している。そのうちの一つが，DNS のセキュリティ対策である。

〔DNS のセキュリティ対策〕

IB システムの DNS 概念図を，図 2 に示す。



注記　設問のために，図の一部を省略している。

図 2　IB システムの DNS 概念図

図2のDNSは，次のセキュリティ対策方針に基づいて構築されている。

・DNS サーバが管理するドメインを，DMZ（外部向けゾーン）と内部セグメント（内部向けゾーン）に分け，それぞれゾーン転送を行う。

・①DMZ の DNS サーバは，キャッシュ機能を無効にしたセカンダリの冗長構成として，DMZ に設置されグローバル IP アドレスを割り当てられた Web サーバの名前解決に使用する。

・内部セグメントの DNS サーバは，プライマリ，セカンダリ，キャッシュをそれぞれ別のサーバ機器で稼働させる。

・内部セグメントのプライマリ DNS サーバには，DNS の問合せが来ないようにし，ゾーン転送の宛先は自行内のセカンダリサーバに限定する。

・内部セグメントのセカンダリ DNS サーバは，内部セグメントに設置されたデータベースサーバの名前解決に使用する。

・FW において，内部セグメントの DNS サーバから DMZ の DNS サーバへの通信は，TCP/UDP ともポート番号 53 番だけを許可する。

DNS の対応を含めた上記のセキュリティ対策を正しく実装し，実効性を確保することが必要である。

次は，侵入検査とインシデント管理に関する，F 氏と G 君の会話である。

G 君：被害が発生してからでは遅いのではないでしょうか。被害を未然に防ぐ対策はないのですか。

F 氏：そうだね。当行では，実際に脆弱(ぜい)性があるかどうか調査するための侵入検査，いわゆる［ オ ］テストを定期的に実施して，セキュリティ対策の状況を評価している。しかし，それだけでなく，平常時の状態をよく監視しておき，被害が発生する前の兆候をつかむことが大切だ。そのためにはインシデント管理が重要だと考えている。また，②外部からの不正アクセスだけでなく，内部から外部への通信にも十分に注意しなければならないね。

G 君：少しでも不審な動きがあったら，事前に定めておいた対応手順に従って，迅速に対応する必要があるということですね。

〔インシデント管理〕

IB システムにおいて，不正侵入などのサイバー攻撃に関わる重大なインシデントが発生した場合，社内のインシデント発見者又は社外からのインシデント連絡を受け付ける担当者が，定められた手順に従ってセキュリティ担当者への連絡を行う。インシデントの連絡を受け付けたセキュリティ担当者は，発生したインシデントの状況を把握し記録した後，必要な対処を実施することが定められている。

IB システムにおいて，サイバー攻撃に関わる重大なインシデントが発生したときのために，X 銀行が定めた対応手順を，図 3 に示す。

＜発見者又は受付担当者の対応＞
(1) 状況把握と記録
(2) 対処方法の確認
(3) セキュリティ担当者への連絡
(4) 対処結果の報告

＜セキュリティ担当者の対応＞
(1) 状況把握と記録
(2) 対処方法の確認
(3) [b]
(4) 原因の特定と対処
(5) システムの復旧
(6) 対処結果の報告

図 3　IB システムのサイバー攻撃に関わる重大なインシデント発生時の対応手順

X 銀行では現在，適切なセキュリティ対策を実施し，インシデント発生時に迅速に対応することによって，IB システムを順調に稼働させている。

設問 1　本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

設問 2　〔サイバー攻撃対策〕について，(1)，(2) に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を答えよ。

(2)　大量のパケットを送信する攻撃として，大きなサイズの ICMP エコー応答を使ったものがある。この攻撃を防御するために，図 1 中の FW がもつべき機能は何か。30 字以内で具体的に述べよ。

設問 3　〔DNS のセキュリティ対策〕について，(1) ～ (3)に答えよ。

(1)　本文中の下線①の対策をとらなかった場合，どのようなセキュリティ上の脆弱性が考えられるか。20 字以内で述べよ。

(2) 本文中のセキュリティ対策を実施した場合の，図 2 中の空欄の DNS サーバと，DNS 問合せ及びゾーン転送について，凡例に従って図 2 を完成させよ。

(3) 本文中の下線②で，内部から外部への不正な通信を発見又は防止するために必要な，FW での対策を二つ挙げ，それぞれ 30 字以内で述べよ。

設問 4 〔インシデント管理〕について，(1)，(2) に答えよ。

(1) 図 3 中の［ b ］は，セキュリティ担当者の対応として必要な，ネットワークに係る作業である。その作業の内容を 15 字以内で答えよ。

(2) 対処結果の報告後，将来発生するインシデントへの対応として，セキュリティ担当者が実施すべき事項がある。その内容を 30 字以内で述べよ。