ネットワークセキュリティ

問２ Check □ □ □ 【2018年秋期 応用情報 問1】

インターネットサービス向けサーバのセキュリティ対策に関する次の記述を読んで，設問１～３に答えよ。

食品販売業を営むＬ社では，社内外の電子メール（以下，メールという）を扱うメールサーバ，商品を紹介するWebサーバ及び自社ドメイン名を管理するDNSサーバを運用している。Ｌ社情報システム部のM部長は，インターネット経由の外部からのサイバー攻撃への対策が重要だと考え，当該サイバー攻撃にさらされるおそれのあるサーバの脆弱性診断を行うように，情報システム部のＮさんに指示した。Ｌ社のサーバなどを配置したDMZを含むネットワーク構成を図１に，各サーバで使用している主なソフトウェアを表１に示す。

なお，Ｌ社のセキュリティポリシでは，各サーバで稼働するサービスへのアクセス制限は，ファイアウォール（以下，FWという）及び各サーバのOSがもつFW機能の両方で実施することになっている。

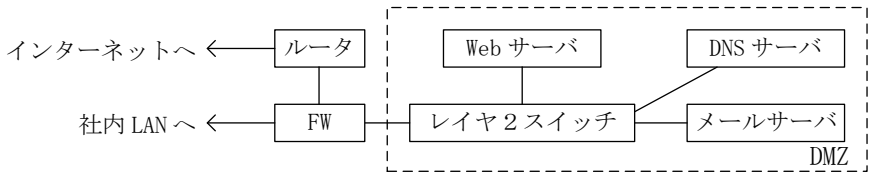

図１　Ｌ社のサーバなどを配置したDMZを含むネットワーク構成

表１　各サーバで使用している主なソフトウェア

サーバ名	ソフトウェア
メールサーバ	OS-A，メールサーバソフトウェア
Webサーバ	OS-B，Webサーバソフトウェア，DBMS， 商品検索ソフトウェア（社外に委託して開発した自社ソフトウェア）
DNSサーバ	OS-A，DNSサーバソフトウェア

〔脆弱性診断の実施〕

Ｎさんは，社外のセキュリティベンダであるＱ社に，メールサーバ，Webサーバ及びDNSサーバの脆弱性診断を実施してもらい，脆弱性診断の内容とその結果を受け取った。Ｑ社が実施した脆弱性診断の内容の抜粋を表２に，Ｑ社から受け取った脆弱性診断結果の抜粋を表３に示す。

表２　Q社が実施した脆弱性診断の内容（抜粋）

項番	項目	実施内容
診１	ポートスキャン	インターネット側から対象サーバに TCP スキャン及び［ a ］スキャンを実施し，稼働しているサービスに関する情報を収集する。
診２	既知の脆弱性に対する診断	使用しているソフトウェアのバージョンなどから既知の脆弱性がないことを確認する。
診３	ソフトウェア設定診断	OS，ミドルウェア，アプリケーションの設定の不備などがないことを確認する。
診４	Web アプリケーション診断	Web アプリケーションについて，［ b ］の不備，Web ページの出力処理の不備などがないことを確認する。

表３　Q社から受け取った脆弱性診断結果（抜粋）

項番	対象サーバ	脆弱性診断の項番	対象ソフトウェア	脆弱性の内容
脆１	メールサーバ	［ c ］	メールサーバソフトウェア	送信ドメイン認証機能が未設定なので，インターネットから届く送信元メールアドレスを偽装したスパムメールを受信してしまう状態であった。
脆２	Web サーバ	診１	OS-B	DBMS に接続するための TCP ポートにインターネットからアクセス可能であった。
脆３		診３	Web サーバソフトウェア	脆弱な暗号化通信方式が使用できてしまう設定であり，情報漏えいのおそれがあった。
脆４		診４	商品検索ソフトウェア	入力値チェックの不備によって，データベースに蓄積された非公開情報が閲覧されるおそれがあった。
脆５	DNS サーバ	診２	DNS サーバソフトウェア	DNS サーバソフトウェアの脆弱性によって，ゾーン情報がリモートから操作可能であった。

〔発見された脆弱性への対策の検討〕

Nさんは，表３の脆弱性診断結果の内容を確認し，発見された脆弱性に対して実施すべき対策の案を検討した。検討結果を表４に示す。

ネットワークセキュリティ

表４　発見された脆弱性に対して実施すべき対策（案）

脆弱性診断結果の項番	実施すべき対策
脆１	メールサーバソフトウェアに送信ドメイン認証機能として［ d ］認証の設定を行う。送信元メールアドレスのドメイン名から DNS に問合せを行い，［ d ］レコードから正規の IP アドレスを調べる。受信したメールの［ e ］IP アドレスと照合して，なりすましの受信メールをフィルタリングする。
脆２	［ f ］と，［ g ］の OS がもつ FW 機能で，DBMS に接続するための TCP ポートを閉塞して，インターネットから DBMS にアクセスできないようにする。
脆３	Web サーバソフトウェアの設定を変更して，脆弱な暗号化通信方式を使用禁止にする。
脆４	SQL 文を組み立てる際に害のあるコードが入力値に含まれていないか十分にチェックして［ h ］を防止する。
脆５	DNS サーバソフトウェアの脆弱性に対応する修正ソフトウェアがリリースされているので，これを適用する。

Ｎさんは，脆弱性診断結果（表３）と，実施すべき対策の案（表４）をＭ部長に報告した。報告を受けたＭ部長は，Ｎさんが検討した表４の脆弱性対策を速やかに実施することと，中長期的な脆弱性対策を検討することを指示した。

〔中長期的な脆弱性対策〕

Ｎさんは，OS やミドルウェアなどの市販ソフトウェアと社外に委託して開発する自社ソフトウェアについて，Ｌ社が中長期的に取り組むべき脆弱性対策の案を検討した。検討結果を表５に示す。

表５　Ｌ社が中長期的に取り組むべき脆弱性対策（案）

市販ソフトウェア	社外に委託して開発する自社ソフトウェア
・サーバで使用しているソフトウェアの製造元・提供元から更新情報を入手する。 ・①社外の関連する組織から脆弱性情報を入手して活用する。 ・運用・保守要員に対するセキュリティ教育を実施し，脆弱性対策への意識を高める。	・ソフトウェア開発の委託先企業との契約に，セキュアコーディングの実施を盛り込む。 ・②ソフトウェア開発の委託先企業のセキュリティ対策の実施状況を確認する。 ・③ソフトウェアの企画・設計段階からセキュリティ機能を組み込むようにセキュリティの専門家を参加させる。

Ｎさんは，表５の脆弱性対策の案を盛り込んだ改善計画を策定し，その結果をＭ部長に報告した。改善計画を確認したＭ部長は，この改善計画を基に具体的な取組みを検討するようにＮさんに指示した。

1　情報セキュリティ

設問１　〔脆弱性診断の実施〕について，(1)，(2)に答えよ。

(1) 表２中の［ a ］，［ b ］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　ARP　　イ　IT 資産管理
ウ　UDP　　エ　XML
オ　インシデント管理　　カ　ウイルス
キ　セッション管理　　ク　ログ管理

(2) 表３中の［ c ］に入れる適切な字句を答えよ。

設問２　〔発見された脆弱性への対策の検討〕について，(1)～(3)に答えよ。

(1) 表４中の［ d ］，［ e ］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　MX　　イ　PTR　　ウ　SMTP　　エ　SPF
オ　送信先　　カ　送信元　　キ　中継先　　ク　中継元

(2) 表４中の［ f ］，［ g ］に入れる適切な字句を，図１中の構成機器の名称で答えよ。

(3) 表４中の［ h ］に入れる適切なサイバー攻撃手法の名称を 15 字以内で答えよ。

設問３　〔中長期的な脆弱性対策〕について，(1)，(2)に答えよ。

(1) 表５中の下線①，②の各対策に該当する項目として適切なものを解答群の中からそれぞれ選び，記号で答えよ。

解答群

ア　インシデント発生時の緊急対応体制を整備する。
イ　公開されている脆弱性情報データベースを確認する。
ウ　実施すべきセキュリティ対策を定めて定期的に監査する。
エ　セキュリティ対策に関する予算を増額する。
オ　リスク分析を定期的に実施して対応計画を立案する。

(2) 表５中の下線③について，表３の項番“脆３”で発見された脆弱性への対策として，ソフトウェアの企画・設計段階からセキュリティの専門家を参加させる狙いを 30 字以内で述べよ。

ネットワークセキュリティ

設問１	(1)	a		b	
	(2)	c			
設問２	(1)	d		e	
	(2)	f		g	
	(3)	h			
設問３	(1)	①		②	
	(2)				