応用情報技術者

上級コース/A/B

見本テキスト

《内容》

- 試験対策テキストⅡ 「システムの利用と開発編」 抜粋
- 午後問題集　抜粋

TAC

応用情報技術者

上級コース/A/B

試験対策テキストII（体験版）

はじめに

応用情報技術者試験(AP)は2009年春期より実施された試験区分であり，従来のソフトウェア開発技術者試験(SW)の後継に位置付けられる試験です。対象者像は，

「高度IT人材となるために必要な応用的知識・技能をもち，
高度IT人材としての方向性を確立した者」

とされています。基本情報技術者試験(FE)で求められる基本的な知識に加え，さらに専門的・詳細な内容を含めた応用的知識が問われることになります。

本書は応用情報技術者試験の出題範囲であるテクノロジ系，ストラテジ系，マネジメント系のうち，テクノロジ系の周辺技術要素であるヒューマンインタフェース，マルチメディア，データベース，ネットワーク，情報セキュリティ，そしてシステム開発に関する分野の知識を網羅しています。その上で，読者の皆さんが効率よく学習が行えるよう，基礎的な用語や考え方を分かりやすく解説するように心がけました。

本書により，読者のみなさんが応用情報技術者試験に合格されることを願ってやみません。

TAC情報処理技術者講座

目　次

第4章

情報セキュリティ

学習テーマ　4－8
ファイアウォール

●ファイアウォールの概念

ファイアウォールは，ネットワークの境界でアクセス制御を行うことにより，インターネットなどの外部ネットワークから，社内LANなどの内部ネットワークを保護する仕組みである。ファイアウォールは，「パケットフィルタリング型」と「アプリケーションゲートウェイ型」に大別されるが，いずれも「どの通信を許可し，どの通信を禁止するか」というルール(ポリシ)に基づいてアクセス制御を行う。

●パケットフィルタリング

パケットフィルタリング型のファイアウォールは，パケットフィルタリングの機能を利用しており，パケットに含まれるIPアドレスやポート番号といった情報をフィルタリングテーブルと照合し，パケットの通過(フォワーディング)や遮断(フィルタリング)を制御する。フィルタリングテーブルのことをアクセス制御リスト(ACL：Access Control List)ともいう。

パケットフィルタリングでは，特定可能な「IPアドレス」と「ポート番号」を用いて，要求パケットと応答パケットの両方を制御する。たとえば，「内部のWebサーバへのHTTP通信のみを許可」する場合，内部のWebサーバへのHTTP要求と，内部のWebサーバからのHTTP応答のみを許可すればよい。仮に，WebサーバのIPアドレスが123.45.67.89であれば，パケットに含まれるヘッダの内容は次のようになる。

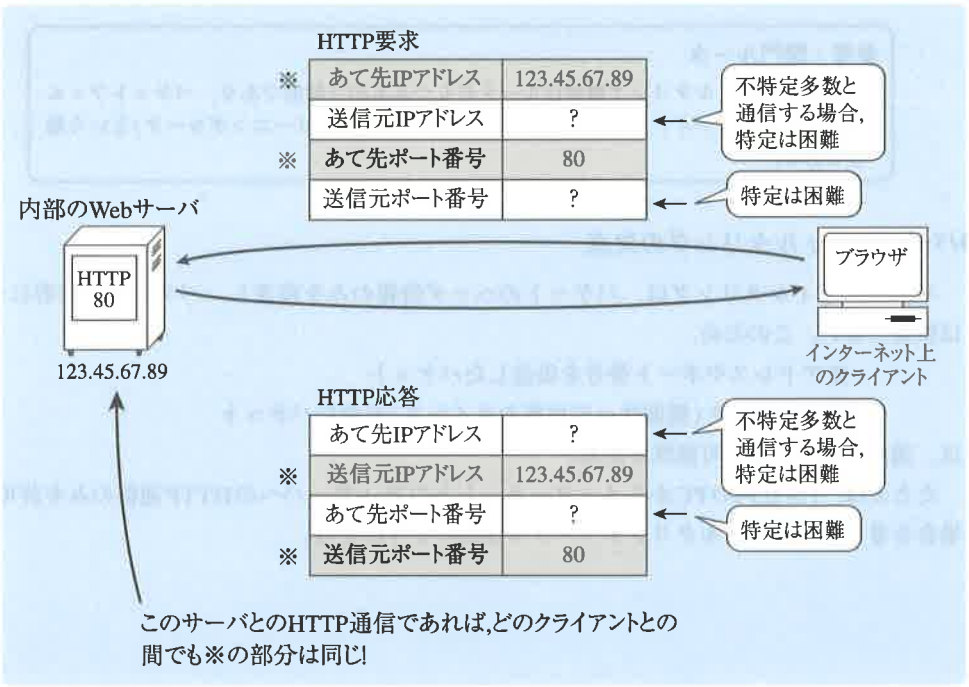
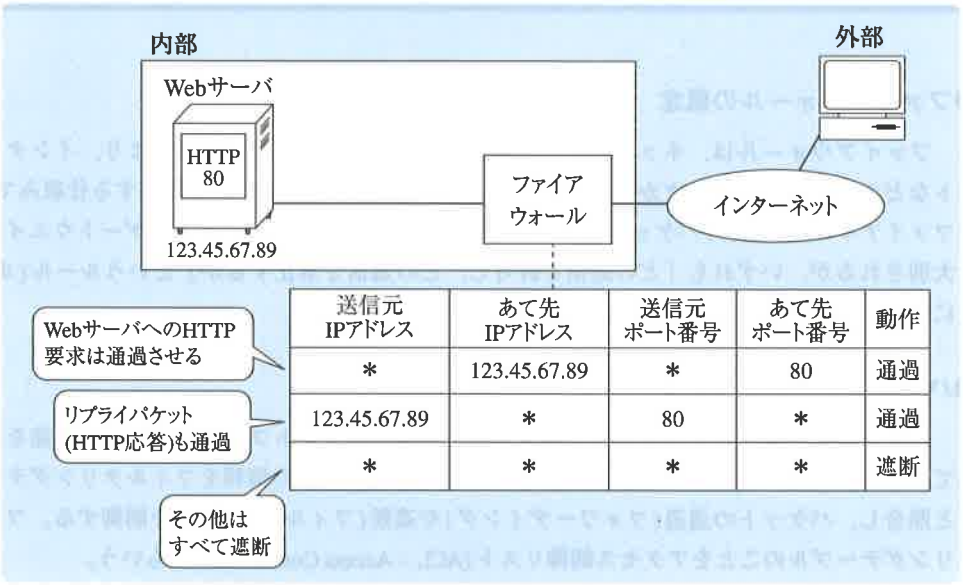


図4.21　HTTP通信におけるヘッダ情報

したがって，フィルタリングテーブルには以下のようなルールを設定すればよい。以下のルールでは，フィルタリングテーブルは上の行から順に検査し，条件に合致する行が見つかった時点で対応する動作を行う。‘*’は制限を行わないことを表す。



送信元 IPアドレス	あて先 IPアドレス	送信元 ポート番号	あて先 ポート番号	動作
*	123.45.67.89	*	80	通過
123.45.67.89	*	80	*	通過
*	*	*	*	遮断

図4.22　フィルタリングテーブルの設定例

このように，パケットフィルタリングによってアクセス制御を行う場合，リプライ(応答)パケットについても設定が必要となる。なお，クライアント側のポート番号として「1024以上(ウェルノウンではないポート番号)」を指定する場合もある。

> **参考：関門ルータ**
> パケットフィルタリング機能はルータがもつ基本的な機能であり，パケットフィルタリング型のファイアウォールのことを関門ルータ(スクリーニングルータ)という場合もある。

●パケットフィルタリングの欠点

パケットフィルタリングは，パケットのヘッダ情報のみを検査し，パケットの内容については検査しない。このため，

・IPアドレスやポート番号を偽造したパケット
・悪意のデータ(脆弱性への攻撃やウイルス)を含むパケット

は，通過させてしまう可能性がある。

たとえば，「自社内のPCからインターネット上のWebサーバへのHTTP通信のみを許可する」場合を考えると，フィルタリングテーブルは次のようになる。

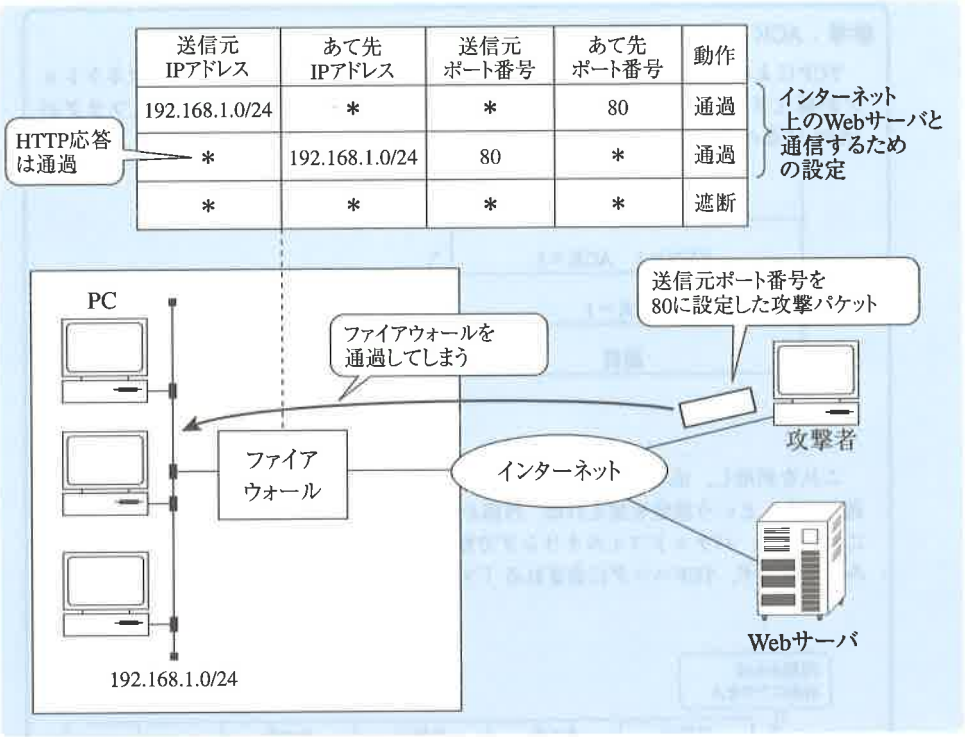


図4.23　攻撃パケットの通過

この例では，送信元ポート番号が80(HTTP応答)の内部向けのパケットは通過させる設定になっている。したがって，送信元ポート番号を80に設定した攻撃パケットは，ファイアウォールがHTTP応答と判断して通過させてしまう。

【ポイント】

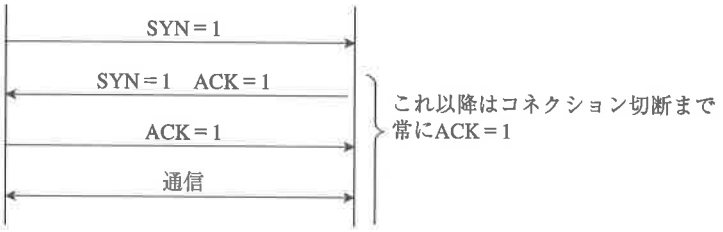
パケットフィルタリング

パケットのヘッダ情報に基づいてパケットの通過／遮断を判断

パケットの内容(データ)に基づく制御は不可能

参考：ACKフラグの利用

TCPによる通信を行う場合は「スリーウェイハンドシェイク」によってコネクションが確立され，コネクションを確立する最初のパケット以外は必ずACKフラグが1(ON)になっている。



これを利用し，応答パケットについては，「ACKフラグが1(ON)のパケットのみ通過させる」という設定を加えれば，外部からのコネクション確立を防ぐことができる。このように，パケットフィルタリングで使用する情報は，IPアドレスとポート番号のみとは限らず，TCPヘッダに含まれる「フラグ」などの情報を用いる場合もある。

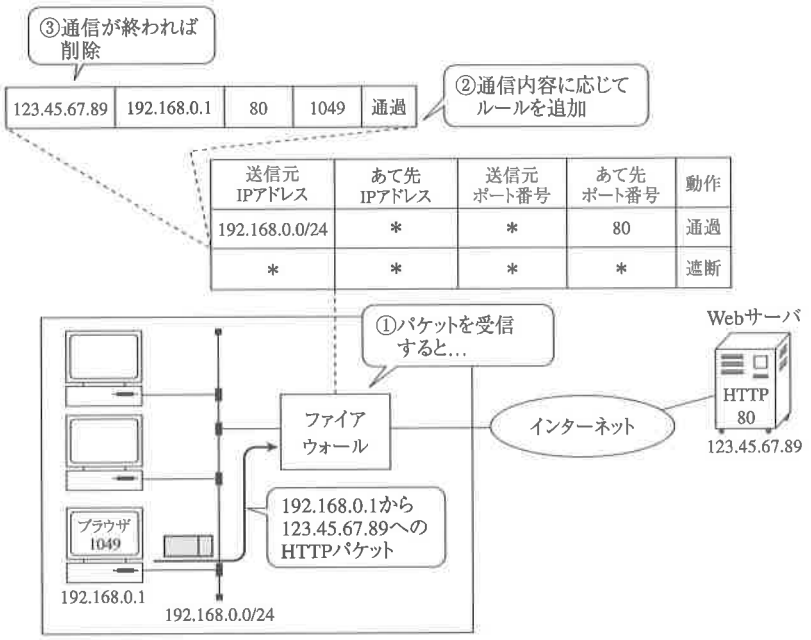
内側からは
自由にアクセス

送信元 IPアドレス	あて先 IPアドレス	送信元 ポート番号	あて先 ポート番号	ACK	動作
192.168.1.0/24	*	*	80	*	通過
*	192.168.1.0/24	80	*	ACK=1	通過
*	*	*	*	*	遮断

外からは
コネクションを
確立させない

参考：動的パケットフィルタリング

動的パケットフィルタリング(ダイナミックパケットフィルタリング)は，通信の発生をきっかけとして，応答パケットが通過できるように「フィルタリングテーブルを動的に書き換える」方式である。これにより，応答パケットのように偽造した攻撃パケットを遮断することが可能となる。



この考え方を応用してTCPセッション(あるいはUDP擬似セッション)の状態を記憶し，セッション状態と矛盾するようなパケットを破棄するような制御をステートフルパケットインスペクションともいう。なお，設定されたフィルタリングテーブルを変更しない方式を静的(スタティック)パケットフィルタリングという。

●アプリケーションゲートウェイ

アプリケーションゲートウェイ(ALG：Application Level Gateway)は，プロキシサーバの機能を利用する方式のファイアウォールである。クライアントからの通信要求を受けると，それが許可された通信であれば，通信を代替することによってアクセス制御を行う。

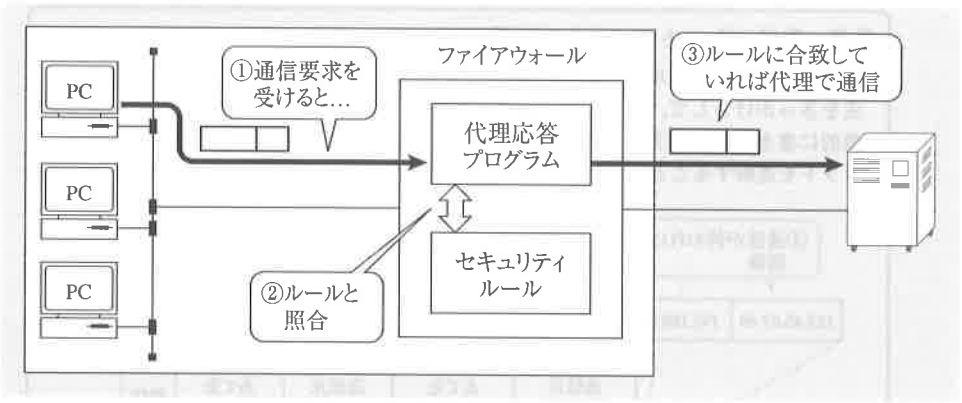


図4.24　アプリケーションゲートウェイ

アプリケーションゲートウェイは，アプリケーション層の情報を参照・解析してアクセス制御を行うことができる。このため，HTTPのパケットに含まれるURLを検査して特定のURLへの接続を禁止する，特定のコマンド(操作)を禁止する，といったパケットフィルタリングでは不可能な制御が可能である。

●ファイアウォールとサーバの配置

ファイアウォールとネットワークの接続構成は様々であり，サーバを設置する領域として，内部セグメント，外部セグメント，DMZ(DeMilitarized Zone：非武装地帯)などがある。現在では，DMZにサーバを配置することが多い。

表4.15　サーバを設置する領域

設置する領域	特徴
外部セグメント	ファイアウォールと外部接続用ルータの間にあるネットワーク。バリアセグメントともいう。サーバが乗っ取られても内部への攻撃はファイアウォールで防げるが，サーバ自体はファイアウォールで保護できない
内部セグメント	ファイアウォールの内側にある保護されたネットワーク。サーバはファイアウォールで保護できるが，サーバが乗っ取られるとすべてのネットワークに被害が及ぶ可能性がある。このため，内部でのみ利用されるサーバ(非公開サーバ)などを配置する
DMZ	外部からも内部からもファイアウォールを介してアクセス可能なネットワーク。サーバをファイアウォールで保護でき，サーバが乗っ取られても内部への攻撃はファイアウォールで防げる

DMZに公開サーバを配置した例を次に示す。ここで，“○”は通信の許可(ただし許可されたものに限定)を表し，“×”は通信の拒否を表す。これらは絶対的なものでなく，システムの構成，サーバの配置，要件，セキュリティポリシなどによって異なる。

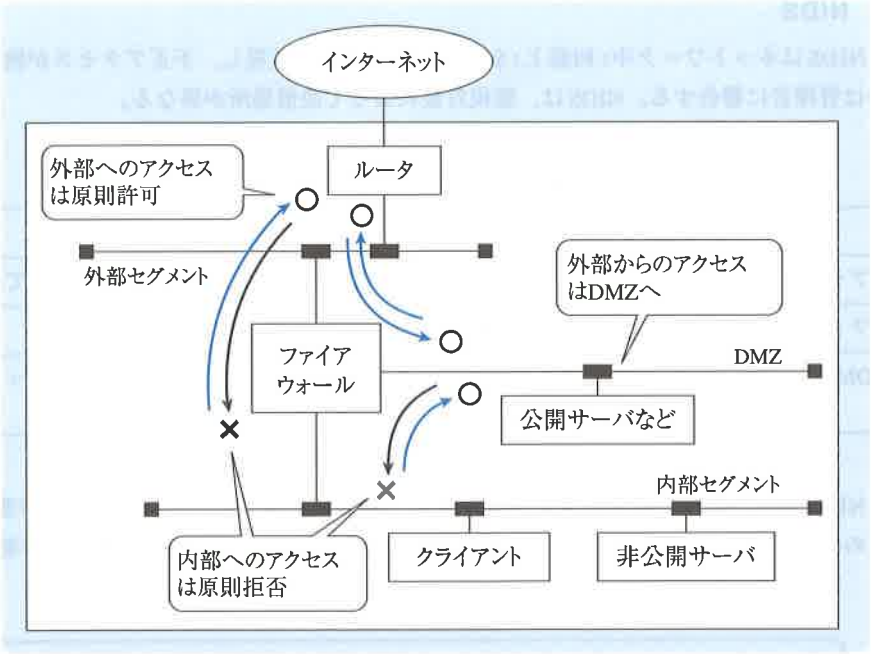


図4.25　DMZを用いたアクセス制御の例

●IDS(侵入検知システム)

ファイアウォールでは，すべての不正なアクセスを遮断できるとは限らない。そこで，IDS(Intrusion Detection System；侵入検知システム)が用いられることもある。IDSは，ネットワーク上を流れるパケットやサーバに対するアクセスなどを監視し，不正アクセスと疑われるアクセスを検出した場合は管理者に警告を発する仕組みである。IDSは，その監視対象によりNIDS(ネットワーク型IDS)とHIDS(ホスト型IDS)に大別される。

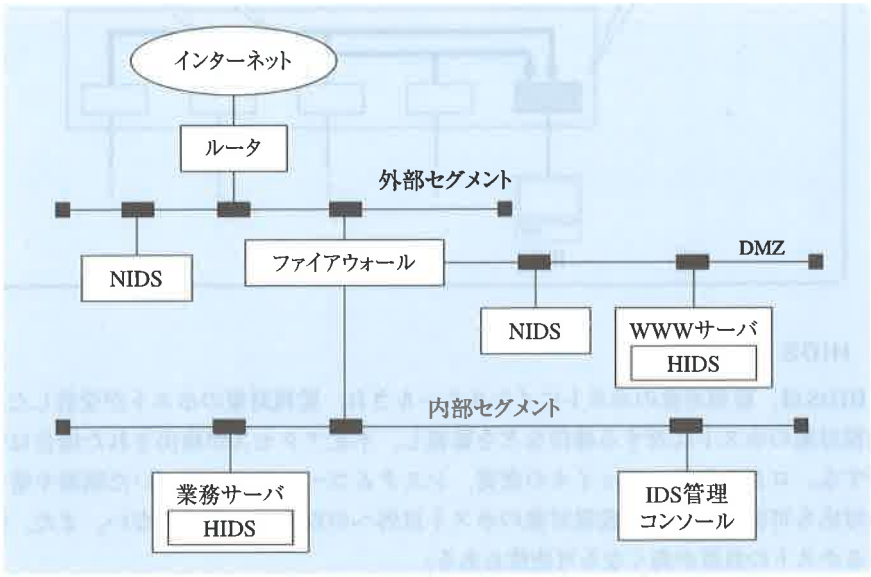


図4.26　IDSの配置

(a)　NIDS

NIDSはネットワーク中(回線上)を流れるパケットを監視し，不正アクセスが検出された場合は管理者に警告する。NIDSは，監視対象によって設置場所が異なる。

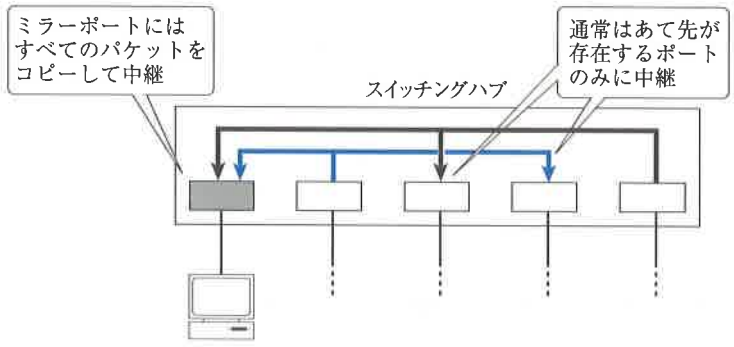
表4.16　IDSの設置場所と監視対象の例

IDSの設置場所	監視対象
ファイアウォールの外側	ファイアウォールがブロックする攻撃を含んだすべての攻撃
ファイアウォールの内側	内部の利用者が行う攻撃
DMZ	ファイアウォールを通過した，公開サーバをターゲットとした攻撃

NIDSは，パケットをリアルタイムで受信・解析・記録するために高い性能が要求される。このため，どのような攻撃を対象とするのかの絞り込みや，配置場所の検討が重要になる。

参考：ポートミラーリング

NIDSは，ネットワーク中を流れるパケットをすべて監視できる場所に設置する。しかし，スイッチングハブはあて先ノードが存在するポートにのみパケットを転送するため，すべてのパケットを監視することが難しい。そこで，NIDSやネットワークアナライザ(LANのパケットを解析する装置)を利用する場合は，ポートミラーリング機能をもつスイッチングハブを利用することが多い。ポートミラーリング機能とは，監視対象のポートを流れるパケットをコピーし，特定のポート(ミラーポート)にも転送する機能である。



(b)　HIDS

HIDSは，監視対象のホストにインストールされ，監視対象のホストが受信したパケットや監視対象のホストに対する操作などを監視し，不正アクセスが検出された場合は管理者に警告する。ログの内容，ファイルの変更，システムコールなどに基づいた制御や暗号化通信への対応も可能であるが，監視対象のホスト以外への攻撃は検出できない。また，監視対象となるホストの負荷が高くなる可能性もある。

(c)　IDSの課題

NIDSとHIDSは，監視対象や監視方法が異なるため，用途に適したIDSを導入し，必要に応じて両者を組み合わせる必要がある。また，攻撃と正常なアクセスを100%区別することは難しく，正常なアクセスを不正アクセスとみなす(偽陽性：false positive)，不正アクセスを正常なアクセスとみなす(偽陰性:false negative)，といった誤りが発生する。これらの誤りに対し，どのように対応するかが重要になる。

参考：IPSとハニーポット

IDSは，原則として不正なアクセスを検出し，通知するだけである。これに対して，不正なアクセスを遮断するシステムをIPS(Intrusion Prevention System：侵入防止システム)という。

また，不正アクセス手法の分析や保護対象のサーバから目を逸らさせることを目的とし，一見すると脆弱に見える(実際は強固に構築された)"おとり"のサーバを用意することがある。このような手法またはおとりのサーバを，ハニーポットという。

参考：ペネトレーションテスト

構築したファイアウォールやIDSといったセキュリティシステムについて，弱点の発見や，実際に機能するかの確認を目的とした擬似侵入テストをペネトレーションテストという。

参考：UTM（Unified Threat Management）

UTM（統合脅威管理）とは，ファイアウォールの機能に加え，後述のVPN装置やアンチウイルス，IDS/IPS，コンテンツフィルタといった総合的なセキュリティ機能を有する装置である。UTMに搭載される機能は製品によって異なるが，少なくともファイアウォール機能を有し，インターネットとの接続境界に設置される製品がほとんどである。

学習テーマ　4－13
アプリケーションセキュリティ

現在では，アプリケーションの脆弱性を狙った攻撃が多い。このため，アプリケーションのセキュリティとして，セキュアプログラミングによる「脆弱性を作りこまないような設計」が重要になる。ここではアプリケーションの脆弱性を狙った攻撃手法と，その対策を解説する。

●SQLインジェクション

SQLインジェクションとは，入力データ中にSQL構文の一部を埋め込んで，任意のSQL文を実行させる攻撃であり，データの不正閲覧やWebサイトの改ざんなどに用いられる。

下の例では，SQL文の意味を変えている(OR '1' = '1' によりすべてのデータが対象となる)が，セミコロン(;)で区切って任意のSQL文を実行することもできる。

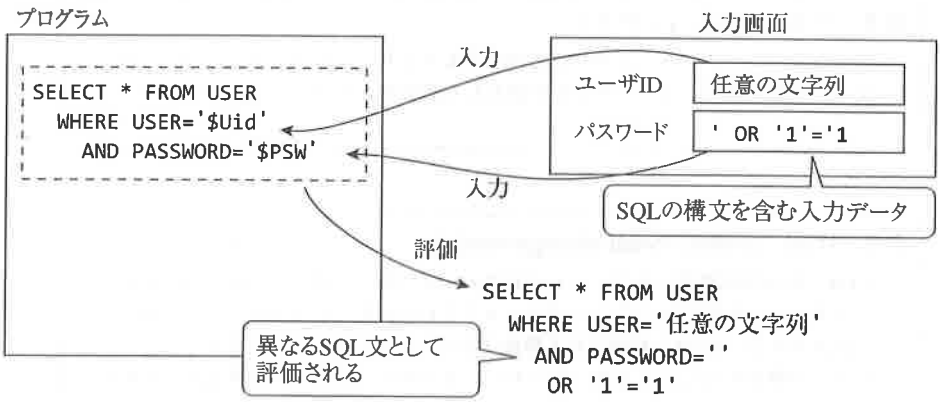


図4.42　SQLインジェクション

SQLインジェクションは入力値を厳密にチェックしないことが原因で発生する。このため，厳密に入力値をチェックして入力値が所定の形式でなければエラー処理を行う(SQLとして処理しない)ことが原則となる。

さらにチェックした入力データは，プリペアドステートメント(準備された文)を用いてSQL文に埋め込む。プリペアドステートメントは，プレースホルダ(値を埋め込む場所)と値を埋め込むためのAPIによって構成される解析済みのSQL文である。内部でバインド機構(プレースホルダに入力データを埋め込む機能)による処理が行われ，入力データは数値または文字列の定数として組み込まれるため，入力データを文字列連結で処理するよりも高い安全性を提供する。

また，プリペアドステートメントが使用できない場合，シングルクォーテーション(')やバックスラッシュ(\)といった特殊記号をエスケープ処理する。DBMSによっては，このためのAPIを提供しているものもあるので，可能であればAPIの利用が望ましい。

> **参考：OSコマンドインジェクション**
> 入力データ中にOSのコマンドを埋め込み，任意のコマンド文を実行させる攻撃をOSコマンドインジェクションという。OSコマンドインジェクションの対策としては，OSのコマンドを呼び出せるような機能(たとえばPerlのopen関数)を利用せず，代わりの機能(sysopen関数など)を利用すればよい。

●クロスサイトスクリプティング

クロスサイトスクリプティング(XSS：Cross Site Scripting)は，入力データをそのまま出力してしまう脆弱サイトを利用し，標的となる利用者のブラウザ上で悪意のスクリプトを実行させる攻撃である。

① 攻撃者は，「脆弱サイトにスクリプトを含む不正な入力データを送信する」といった悪意のハイパリンクを含むWebページ(またはメール)を用意する。

② 利用者がそのWebページを閲覧し，ハイパリンクをクリックすると，スクリプトを含む不正な入力データが脆弱サイトに送信される。

③ 脆弱サイトによって悪意のスクリプトを含んだWebページが生成され，利用者に返される。

④ ブラウザは，受信したページに含まれる悪意のスクリプトを実行する。

この結果，クッキーを盗まれることによるセッションの乗っ取り(なりすまし)や偽造ページの表示(フィッシング)といった被害が考えられる。

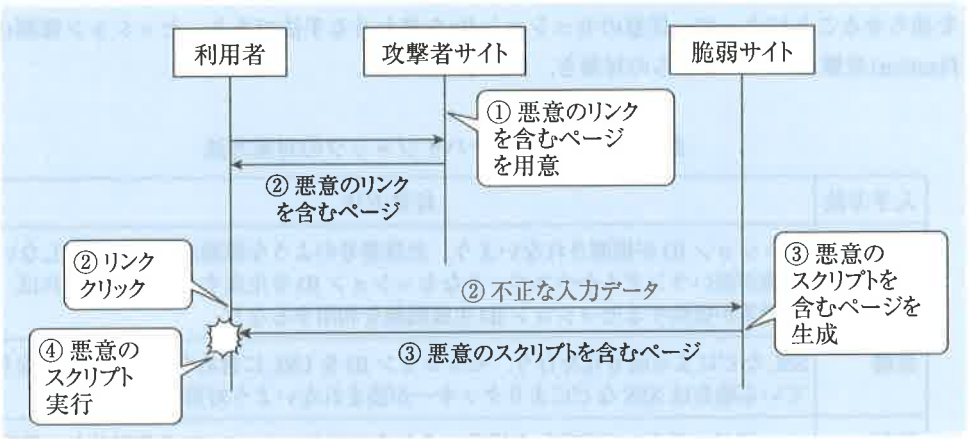


図4.43　クロスサイトスクリプティング

クロスサイトスクリプティングは，入力データに含まれるHTMLのタグを，そのまま出力結果のHTMLに含めてしまう脆弱性を利用する。具体的には，入力データに<script>タグなどを含めることによって，任意のスクリプトを含んだWebページを生成させる。したがって，“<”や“>”といった制御文字をエスケープ処理するサニタイジング(無害化)が有効である。たとえば，<script>という文字列を『<script>』に変換すれば，HTML上で『<script>』という文字が表示される。すなわち，<script>タグとはみなされず，スクリプトは実行されない。

●セッションハイジャック

多くのWebアプリケーションでは，利用者(セッション)を識別するために，セッション識別子を利用する。これをセッションIDという。セッションIDはWebアプリケーション側に提示され，Webアプリケーションはセッション IDからセッションを識別して処理を行う。このセッションIDを攻撃者が入手すると，攻撃者は利用者になりすますことができてしまう。このような攻撃をセッションハイジャックという。

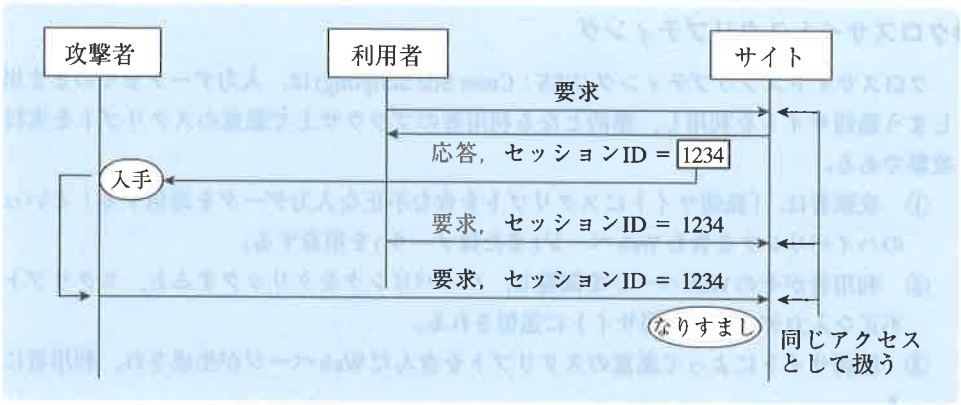


図4.44　セッションハイジャック

攻撃者がセッションIDを入手するためには，セッションIDの推測，盗聴，強制のいずれかが行われる。セッションIDの強制とは，攻撃者自身が生成したセッションIDを含むハイパリンクを辿らせることによって，任意のセッションIDを使わせる手法であり，セッション強制(Session Fixation)攻撃という。これらの対策を，次に示す。

表4.21　セッションハイジャックの対策方法

入手方法	対策方法
推測	セッションIDが推測されないよう，会員番号のような推測が可能な値としない，桁数が長いランダムかつユニークなセッションIDを生成する。可能であれば，処理系が提供するセッションID生成機能を利用するなど
盗聴	SSLなどによる暗号化を行う，セッションIDをURLに含めない，クッキーを用いている場合はXSSなどによりクッキーが盗まれないよう対策するなど
強制	ユーザがログインに成功した場合，それまでのセッションIDを無効化し，新規のセッションIDを発行するなど

Webサーバにセッション IDを送る場合，一般的には次のような手段が考えられる。

・GETメソッドでURLにセッションIDを格納する
・POSTメソッドでhiddenフィールドにセッションIDを格納する
・cookieにセッションIDを格納する

このうち，GETメソッドの利用は極力控えるべきである。なぜなら，Webサーバに対して，直前に訪問したWebサイトのURL(Referer)を送信する機能によって，URLは第三者に知られや

すいという特徴をもつためである。このため，URLには誰に知られても問題ないような情報のみを格納することが原則となる。

また，POSTメソッドやcookieを用いた場合でも，盗聴やcookieの窃取によってセッションIDが第三者に知られる可能性は十分にある。このため，セッションIDを推測困難な値にする，セッションIDの有効期限を極力短くする，などの対策も重要になる。

●ディレクトリトラバーサル

パラメタとしてファイル名を受け取るWebプログラムに，「../../etc/passwd」のような上位階層を含むパラメタを渡してサーバ内の任意のファイルを読み出す攻撃をディレクトリトラバーサル攻撃という。

ディレクトリトラバーサル攻撃の対処方法としては，そもそもパラメタを用いてサーバ内のファイルを直接指定する必要があるのか，他の代替手段がないのか，といった設計段階からの検討が重要になる。仮にファイルを直接指定せざるを得ない場合は，ディレクトリ名を固定した上で，ファイル名にパスが含まれないような実装が望ましい。

●CSRF

セッションIDなどを用いてログイン状態を維持するようなWebアプリケーションで，攻撃者がハイパリンクなどを利用して，ログイン中の利用者に意図しないリクエストを送信させる攻撃を，CSRF(Cross Site Request Forgeries；クロスサイトリクエストフォージェリ)という。攻撃を受けた利用者は，商品の購入，各種設定の変更(コミュニティからの退会やパスワードの変更など)，掲示板への書込みといった意図しない操作を実行してしまう。

CSRFの対策方法としては，セッションIDに加えて予測困難な第二セッションIDを生成し，正常なページ遷移を辿らない場合(正当な手順を飛ばした処理)は無効とする方法や，利便性は低下するが要所で認証を要求する方法などがある。

参考：WAF

ここまで攻撃手法と，その対策方法を紹介した。これ以外にも，Webアプリケーションの脆弱性を利用する攻撃に対する対策方法として，WAF(Web Application Firewall)の利用が挙げられる。WAFは，脆弱性を悪用した攻撃を検出し，それらの攻撃からWebアプリケーションを保護する仕組みであり，攻撃による影響を低減する。WAFがもつ機能には，次のようなものがある。

検査機能	HTTP要求及びHTTP応答を検査し，攻撃を検出する機能。HTTP要求にSQL文の一部が含まれている，HTTP応答に個人情報が含まれているなど
処理機能	検査機能によって検出された攻撃を処理する機能。通信の遮断，エラーページの送信，不正部分の書換えなど
ログ機能	WAFの動作や検査結果を記録する機能

なお，WAFでは，定義されたパターンを用いて機械的に通信内容を検査する。このため，正常な通信を防御する(偽陽性：false positive)，攻撃を正常な通信とみなす(偽陰性：false negative)，といった誤りがある点に注意する。

応用情報技術者

上級コース/A/B

午後対策問題集（体験版）

はじめに

この問題集は，弊社刊「応用情報技術者試験対策テキストⅠ・Ⅱ・Ⅲ」の各学習項目に対応させて作成された問題集です。応用情報技術者試験の午後試験出題範囲である各分野(テクノロジ系，マネジメント系，ストラテジ系)の問題を，広く多数掲載しています。

本書は，過去の情報処理技術者試験において出題された午後問題で構成されています。実際の応用情報技術者試験の出題形式に合わせ，テーマごとに問題を集めて掲載しています(出典は目次の後)。

試験に合格するためには，テキストによる知識のインプットだけではなく，問題演習によるアウトプット(力試し)が非常に重要になります。問題を解き，間違えた問題のジャンルについては学習しなおして再度挑戦するという学習サイクルを身に付けましょう。

本書が，応用情報技術者試験の合格のお役に立てることを願ってやみません。

2013年11月

TAC情報処理技術者講座

目　次

出典一覧

第1章　プログラミング

問1	平成21年春期本試験　問2
問2	平成21年秋期本試験　問2
問3	平成22年春期本試験　問2
問4	平成22年秋期本試験　問2
問5	平成23年春期本試験　問2
問6	平成23年秋期本試験　問2

第2章　システムアーキテクチャ

問1	平成21年春期本試験　問4
問2	平成21年秋期本試験　問4
問3	平成22年春期本試験　問4
問4	平成22年秋期本試験　問4

第3章　データベース

問1	平成21年春期本試験　問6
問2	平成21年秋期本試験　問6
問3	平成22年春期本試験　問6
問4	平成23年春期本試験　問6

第4章　ネットワーク

問1	平成21年秋期本試験　問5
問2	平成22年春期本試験　問5
問3	平成23年春期本試験　問5
問4	平成23年秋期本試験　問5

第5章　情報セキュリティ

問1	平成21年春期本試験　問9
問2	平成21年秋期本試験　問9
問3	平成22年春期本試験　問9
問4	平成22年秋期本試験　問9
問5	平成23年春期本試験　問9
問6	平成23年秋期本試験　問9

第6章　情報システム開発

問1	平成21年春期本試験　問8
問2	平成21年秋期本試験　問8
問3	平成22年春期本試験　問8
問4	平成22年秋期本試験　問8

第7章　組込みシステム開発

問1	平成21年春期本試験　問7
問2	平成22年春期本試験　問7
問3	平成22年秋期本試験　問7
問4	平成23年春期本試験　問7

第8章　プロジェクトマネジメント

問1	平成21年秋期本試験　問10
問2	平成22年春期本試験　問10
問3	平成22年秋期本試験　問10
問4	平成23年秋期本試験　問10

第9章　ITサービスマネジメント

問1	平成21年春期本試験　問11
問2	平成22年春期本試験　問11
問3	平成22年秋期本試験　問11
問4	平成23年春期本試験　問11

第10章　システム監査

問1	平成21年春期本試験　問12
問2	平成21年秋期本試験　問12
問3	平成22年秋期本試験　問12
問4	平成23年春期本試験　問12

第11章　経営戦略と情報戦略

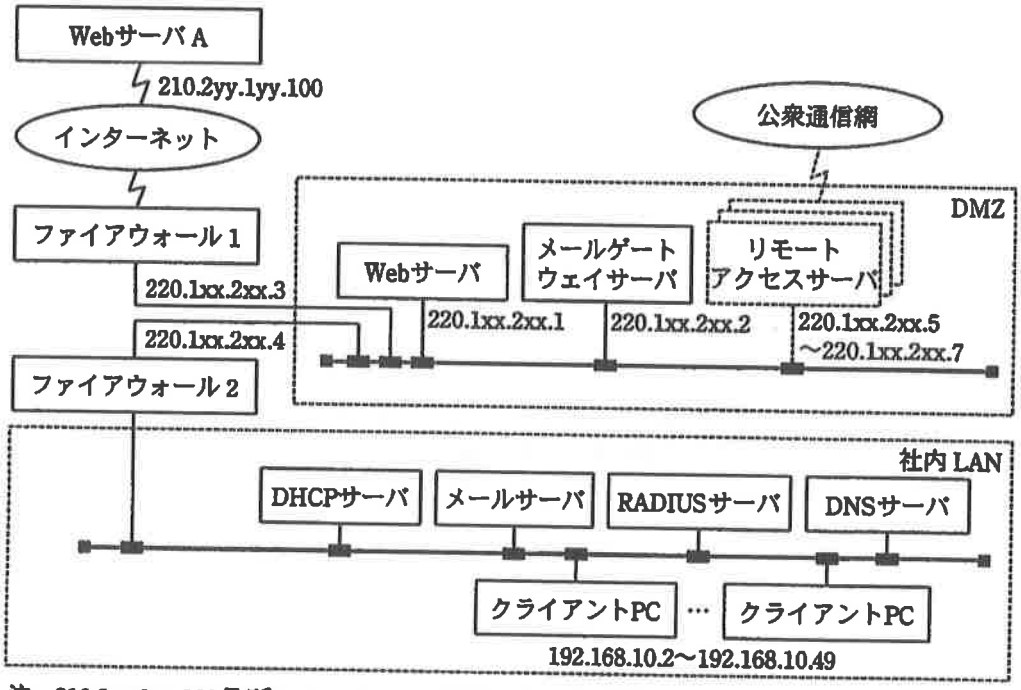
問1	平成21年春期本試験　問3
問2	平成22年春期本試験　問3
問3	平成23年秋期本試験　問1
問4	平成21年秋期本試験　問1
問5	平成22年春期本試験　問1
問6	平成22年秋期本試験　問3

問題編

第５章　情報セキュリティ

問1　ファイアウォールの設定に関する次の記述を読んで，設問1～4に答えよ。

Q社のネットワーク構成を図1に示す。なお，図中のリモートアクセスサーバは，現在はまだ設置されていない。また，WebサーバAは，外部のサーバである。



注　210.2yy.1yy.100及び220.1xx.2xx.1～220.1xx.2xx.7はIPアドレスである。

図1　Q社のネットワーク構成

Q社では，次の情報セキュリティポリシに基づいて，ファイアウォールの設定などを行っている。

〔情報セキュリティポリシ〕

・インターネットからは，自社のWebサーバ及びメールゲートウェイサーバあての通信のほか，社内LANからインターネット上のWebサーバを参照したときの応答の通信を通過させる。

・社内LANからは，電子メールを送受信するための通信及びインターネット上のWebサイトを参照するための通信だけを許可する。

・インターネットへ送信する電子メールは，メールサーバからメールゲートウェイサーバを経由して送信される。また，インターネットから受信した電子メールはメールゲートウェイサーバを経由し，直ちにメールサーバに転送される。
・ファイアウォール1及び2のアクセスログを毎日チェックし，異常なアクセスがあれば，その対応策を検討するとともに，ファイアウォールの設定変更などを行う。

ファイアウォール1及び2における通信制御のための設定は，次のとおりである。

〔ファイアウォール1の設定〕

(1)　静的パケットフィルタリング機能

インターネットから［　a　］への通信，及び社内LANからインターネットへの通信は，いずれも送信先IPアドレス，送信先ポート番号及びプロトコルを参照して，アクセスを制御している。また，［　b　］から社内LANへの通信は，次の動的パケットフィルタリング機能によって通過させるもの以外，すべて遮断する。

(2)　動的パケットフィルタリング機能

社内LAN上のクライアントPCから，TCPを使ったインターネット上のWebサイト参照に関しては，フィルタリングテーブルが表のように設定されている。クライアントPCから図1のWebサーバAを参照した際の応答のパケットを通過させるために，例えばクライアントPC（192.168.10.5）からフィルタリングテーブルの行番号10によって許可されるパケットを送信すると，動的パケットフィルタリング機能では行番号10と行番号20の間に行番号15の行を挿入する。行番号15の行は，TCPセッションの終了パケット受信後に削除する。

表　フィルタリングテーブル（抜粋）

番号	向き	送信元IPアドレス	送信先IPアドレス	プロトコル	送信元ポート番号	送信先ポート番号	処理
10	OUT	c	anywhere	TCP	any	80	許可
20	OUT/IN	anywhere	anywhere	TCP	80	any	遮断
15	IN	d	220.1xx.2xx.4	TCP	80	1024	許可

注　anywhereは任意のIPアドレス，anyは任意のポート番号，“OUT/IN”はOUTとINのいずれかを，それぞれ意味している。

(3) ステートフルインスペクション機能

社内 LAN からインターネット上のサイトを参照したときの応答のパケットを通過させる際に，パケットの順番を管理する TCP ヘッダのシーケンス番号の妥当性を確認して通過させる。これによって，［ e ］の脅威からネットワークを防御する。

〔ファイアウォール 2 の設定〕

(1) 静的パケットフィルタリング機能

メールゲートウェイサーバとメールサーバの間の通信は，双方向とも許可する。それ以外の通信は，［ f ］及び DMZ 上のサーバから［ g ］へは，次の動的パケットフィルタリング機能によって通過させるもの以外，すべて遮断し，［ g ］からは，いずれも送信先 IP アドレス，送信先ポート番号及びプロトコルを参照して許可するか遮断するかを決定する。

(2) 動的パケットフィルタリング機能

ファイアウォール 1 の設定と同様の設定を適用する。

(3) IP アドレスの変換機能

社内 LAN からインターネットへの同時複数通信を可能にするために，NAPT を利用して，プライベート IP アドレスからグローバル IP アドレスへ変換する。これは，グローバル IP アドレス数の不足を解消するとともに，［ h ］という効果も実現している。

〔アクセスログの監視記録〕

アクセスログを基に，ある日にファイアウォール 1 で遮断された通信を送信元 IP アドレス別に分析し，図 2 のようなレポートを作成した。この結果から，［ i ］の危険性が認められるので，ファイアウォールの設定を見直した。

送信元IPアドレス	送信先IPアドレス	プロトコル	送信先ポート番号	受信件数
220.2zz.1zz.40	220.1xx.2xx.1	TCP	1	210
220.2zz.1zz.40	220.1xx.2xx.1	TCP	2	212
220.2zz.1zz.40	220.1xx.2xx.1	TCP	3	211
⋮	⋮	⋮	⋮	⋮
220.2zz.1zz.40	220.1xx.2xx.1	TCP	65534	211
220.2zz.1zz.40	220.1xx.2xx.1	TCP	65535	210

図 2 アクセスログ分析レポート

〔携帯電話を経由したリモートアクセス接続計画〕

Q社では，営業活動の効率を上げるために，営業員にノートPCを携帯させ，携帯電話を経由して社内LANにアクセスできる環境を構築することを計画している。その際のセキュリティ対策は，次のとおりである。

・複数の営業員からの同時接続を可能にするために，ダイヤルアップ接続に利用するリモートアクセスサーバをDMZに3台設置する。同サーバには認証機能をもたせず，社内LANに設置されている［ j ］で認証を行う。これによって，認証情報の安全性を確保するとともに，［ k ］を可能にする。

・ファイアウォール2では，リモートアクセスサーバと［ j ］及びリモートアクセスを許可された社内LAN上のサーバとの通信を許可するように，パケットフィルタリングの設定を追加する。

設問1　本文中の［ a ］，［ b ］，［ f ］，［ g ］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。解答は重複して選んでもよい。

解答群

ア　DMZ　　イ　インターネット　　ウ　社内LAN

設問2　本文中の［ c ］，［ d ］，［ j ］に入れる適切な字句を答えよ。なお，［ j ］には，図1中にあるサーバの名前が入る。

設問3　本文中の［ h ］には，社内LANのセキュリティを維持するのに有効な機能に関する字句が，［ k ］には，［ j ］が果たすべき役割に関する字句がそれぞれ入る。［ h ］に入れる適切な字句を30字以内で，［ k ］に入れる適切な字句を20字以内で答えよ。

設問4　本文中の［ e ］と［ i ］に入れる攻撃手法を解答群の中から選び，記号で答えよ。

解答群

ア　IPスプーフィング　　イ　SQLインジェクション

ウ　クロスサイトスクリプティング　　エ　パスワードクラッキング

オ　ポートスキャン

問5　サーバへのサイバー攻撃対策に関する次の記述を読んで，設問1～3に答えよ。

D社はおもちゃを扱う中堅商社であり，取扱商品を紹介するためにWebサーバやデータベースサーバ（DBサーバ）などを自社で運用している。D社のネットワーク構成を図1に，各サーバの役割を表1に示す。

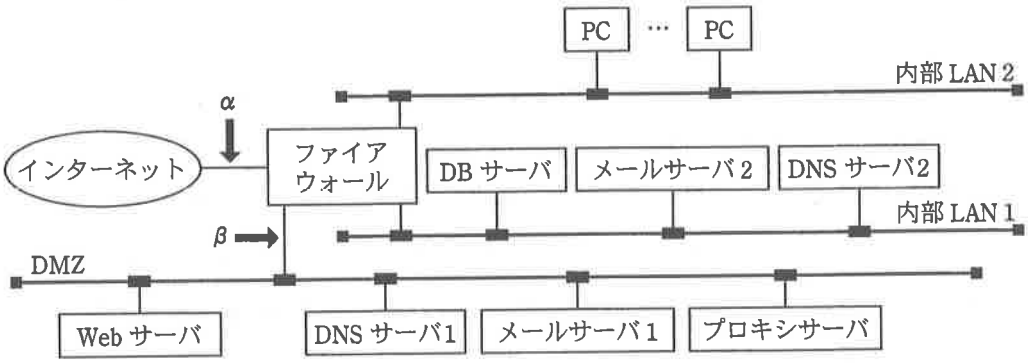


図1　D社のネットワーク構成

表1　各サーバの役割

サーバ名（ホスト名）	役割
DBサーバ	取扱商品の情報を格納し，Webサーバからのリクエストに応じて必要な情報を渡す。
DNSサーバ1	自社ドメインを管理し，インターネットからの問合せに応答する。
DNSサーバ2	自社内のホスト情報を管理し，社内からの問合せに応答する。
Webサーバ	DBサーバにアクセスすることによって，取扱商品をインターネット向けに紹介する。
メールサーバ1	自社あてのメールをインターネットから受け取り，メールサーバ2に転送する。社外あてのメールをメールサーバ2から受け取り，インターネットに転送する。
メールサーバ2	自社あてのメールをメールサーバ1から受け取る。社外あてのメールをメールサーバ1に転送する。PCからのメール送受信要求を受け付ける。
プロキシサーバ	PCからの社外へのWebアクセスを中継する。

あるとき，D社の顧客から“Webサイトが表示されない”と問合せがあった。原因を調査したところ，Webサーバが反応しない状態であったので，Webサイトの運営を一時中止して原因を探った。その結果，各サーバに対して，次のサイバー攻撃が行わ

れていたことが判明した。

【サイバー攻撃 1】Web サーバに対して，Web ページを表示するためのリクエストが大量に送られ，CPU とメモリの使用率が許容限度を超えてしまっていた。

【サイバー攻撃 2】DB サーバにアクセスするプログラムの不備を利用して，データベース上の情報に不正にアクセスしようとした形跡が，Web サーバにあった。

【サイバー攻撃 3】DNS プログラムが確保したメモリサイズを超えた入力を与えて，管理者権限を奪おうとした形跡が，DNS サーバ 1 にあった。

【サイバー攻撃 4】使用可能なサービスを探した形跡が，DMZ 内の各サーバにあった。

D 社では判明したサイバー攻撃に対応するために，ファイアウォールの設定を変更するとともに，ネットワーク型 IDS（Intrusion Detection System，侵入検知システム）を導入することにした。

〔ファイアウォールの設定変更〕

ファイアウォールの新しいフィルタリングルールを表 2 に示す。フィルタリングルールの設定は，次の方針で行うことにした。

・インターネット以外のあて先は，ホスト名で指定する。
・必要なサービスだけを通過させる。

なお，表 2 で用いるフィルタリングルールの記述方法は，次のとおりである。

・通信パケットの送信元，あて先及びサービスの組合せによって，許可又は拒否の動作を指定することができる。
・送信元，あて先には個別のホスト名又は“インターネット”，“DMZ”，“内部 LAN1”，“内部 LAN2”のネットワーク名又は“すべて”が指定できる。
・サービスにはポート番号（複数指定可）又は“すべて”が指定できる。ポート番号は，SMTP は 25，DNS は 53，HTTP は 80，POP3 は 110，DB サーバへのアクセスは 1521，プロキシサーバへのアクセスは 8080 とする。
・項番が小さいものから順に調べて，最初に一致したルールが適用される。

表2　ファイアウォールの新しいフィルタリングルール

項番	送信元	あて先	サービス	動作
1	内部 LAN2	メールサーバ 2	25，110	許可
2	内部 LAN2	DNS サーバ 2	53	許可
3	内部 LAN2	a	b	許可
4	メールサーバ 2	メールサーバ 1	25	許可
5	メールサーバ 1	メールサーバ 2	25	許可
6	Web サーバ	c	d	許可
7	メールサーバ 1	インターネット	25	許可
8	プロキシサーバ	インターネット	すべて	許可
9	インターネット	Web サーバ	80	許可
10	インターネット	e	f	許可
11	インターネット	DNS サーバ 1	53	許可
12	すべて	すべて	すべて	拒否

〔ネットワーク型 IDS の導入〕

D 社では，早期にサイバー攻撃を検知するために，ネットワーク型 IDS を図 1 の α の位置に設置した。設置した IDS の概要は，次のとおりである。

・不正侵入の特徴的なパターンをシグネチャとして事前に登録し，検知した脅威の種類を示すシグネチャの識別子，脅威の名称，詳細な通信内容などをログに記録するとともに，管理者あてに警告メールで通知する機能をもつ。

・検知されるサイバー攻撃には，4 段階の優先度（優先して対応する必要性の度合い）が付与されている。優先度は，優先度 1 が最も高く，優先度 4 が最も低い。

D 社で判明したサイバー攻撃 1～4 に対応する優先度の初期値は，表 3 のとおりである。

表3　D社で判明したサイバー攻撃1～4に対応する優先度の初期値

サイバー攻撃の種類	優先度の初期値
サイバー攻撃1	2
サイバー攻撃2	1
サイバー攻撃3	1
サイバー攻撃4	2

D社では，IDSの優先度の設定は初期値のままとし，優先度が1，2のものを管理者に警告メールで通知する設定で，IDSの試験運用を開始した。

試験運用を開始してすぐに，IDSから管理者あてに警告メールが大量に送られるようになった。警告メールが多いと，管理者が重要な警告を見落とすおそれがあることから，D社ではIDSの導入効果を維持したまま警告メールの件数を少なくするために，①IDSの設置位置を図1のβの位置に変更した。

設問1　サイバー攻撃1～4について，その名称を解答群の中から選び，記号で答えよ。

解答群

ア　DoS攻撃　　イ　SQLインジェクション

ウ　ソーシャルエンジニアリング　　エ　トロイの木馬

オ　バッファオーバフロー攻撃　　カ　ポートスキャン

設問2　D社で実施したファイアウォールの設定変更について，表2中の［ a ］～［ f ］に入れる適切な字句を答えよ。

設問3　IDSから管理者あてに送られる警告メールの大量発生後に，D社が実施した対策について，(1)，(2)に答えよ。

(1)　本文中の下線①の対策について，警告メールが減少する理由を35字以内で述べよ。

(2)　本文中の下線①の対策の結果，警告メールが最も効果的に減少すると考えられるサイバー攻撃の種類をサイバー攻撃1～4から選び，番号で答えよ。

解答・解説編

第５章　情報セキュリティ　解答・解説

問1

解答

TAC解答例

設問1	a	ア	b	イ	f	イ	g	ウ
設問2	c	220.1xx.2xx.4			d	210.2yy.1yy.100		
	j	RADIUSサーバ						
設問3	h	社内LANのクライアントのアドレス情報を						
		隠ぺいする						
	k	認証情報の一元管理						
設問4	e	ア	i	オ				

解説

ファイアウォール1，2を通過させる通信の種類に注目して，問題文で提示されている情報セキュリティポリシをまとめてみると，以下のようになる。

(ファイアウォール1を通過させる通信)

インターネット側からDMZ側へ送られてくるパケットの向きがIN，DMZ側からインターネット側へ送るパケットの向きがOUTとなる。

・IN

Webサーバ，メールゲートウェイサーバあてのパケット

インターネット上のWebサーバから社内LANへのHTTP応答パケット

・OUT

Webサーバ，メールゲートウェイサーバからのパケット

社内LANからインターネット上のWebサーバへのHTTP要求パケット

(ファイアウォール2を通過させる通信)

DMZ側から社内LANへ送られてくるパケットの向きがIN，社内LANからDMZ側へ送るパケットの向きがOUTとなる。

・IN

メールゲートウェイサーバ(DMZ)からメールサーバ(社内LAN)へのパケット

インターネット上のWebサーバから社内LANへのHTTP応答パケット

・OUT

メールサーバ(社内LAN)からメールゲートウェイサーバ(DMZ)へのパケット

社内LANからインターネット上のWebサーバへのHTTP要求パケット

設問1

静的パケットフィルタリングとは，管理者によって(手動で)フィルタリングルールを固定的にフィルタリングテーブルに設定しておく方法である。あらかじめ，送信元や送信先，プロトコル，通過の許可／拒否が決まっている場合に用いる。

一方，動的パケットフィルタリングとは，通信状態に応じて，フィルタリングルールをフィルタリングテーブルに新たに追加したり削除したりする方法である。要求のあった通信に対する応答のみを通過させる場合や，特定のホストに対するサービス不能攻撃の回避などに利用する。

a，bについて

ファイアウォール1を通過する通信は，

①インターネット ～ DMZ(Webサーバ，メールゲートウェイサーバ) 間の通信

②インターネット ～ 社内LAN(PC) 間のHTTP通信

である。

①については，通信するサーバとそのサーバが使用するポート番号が限られているので，双方向を静的パケットフィルタリングで適切に対応できる。

次に，②について考える。OUT方向，すなわちPCからのHTTP要求パケットについては，

送信元IPアドレス：PCのIPアドレスを変換した結果(後述の空欄cの解説参照)

送信先IPアドレス：anywhere

送信元ポート番号：any

送信先ポート番号：80

という許可設定を行えばよく，静的パケットフィルタリングで適切に対応できる。一方，IN方向，すなわちインターネット上のWebサーバからのHTTP応答パケットは，静的パケットフィルタリングで対応しようとすると，上記の送信元／送信先を逆にした

送信元IPアドレス：anywhere

送信先IPアドレス：PCのIPアドレスを変換した結果

送信元ポート番号：80

送信先ポート番号：any

のように許可設定するしかない。しかし，この設定では送信元IPアドレス，送信先ポート番号をともに特定できないため，正当なHTTP応答パケットだけでなく，

「不特定のホストからの」

「あらゆるポートあてのパケット」

を，外から内に向けて通過させてしまうことになる。

したがって，インターネット上のWebサーバからの応答パケットの通過については，動的パケットフィルタリングを用いることが望ましい。

以上をまとめると，

静的パケットフィルタリング機能で以下をアクセス制御

・インターネット ～ DMZ(Webサーバ，メールゲートウェイサーバ) 間の通信

・社内LANからインターネット(上のWebサーバ)への通信

動的パケットフィルタリング機能で以下をアクセス制御

・インターネットから社内LANへの通信

とすればよい。よって，各空欄は

空欄a … DMZ

空欄b … インターネット

となる。

f，gについて

ファイアウォール2を通過する通信は，

①メールゲートウェイサーバ ～ メールサーバ 間の通信

②インターネット ～ 社内LAN(PC) 間のHTTP通信

である。

①については，問題文中の〔情報セキュリティポリシ〕の記述にあるように，メールゲートウェイサーバとメールサーバが相互に通信を行うので，この通信を許可する。

②については，ファイアウォール1での検討と同様，

OUT方向については静的パケットフィルタリング

IN方向については動的パケットフィルタリング

でアクセス制御を行う。問題文の記述を用いて言い換えると，

(IN方向)

インターネット及びDMZ上のサーバから社内LANへは，

動的パケットフィルタリング機能によって通過させるもの以外，すべて遮断

(OUT方向)

社内LANからは，

いずれも送信先IPアドレス，送信先ポート番号及びプロトコルを参照して

許可するか遮断するかを決定

という制御を行うべきである。

以上より，各空欄は

空欄f … インターネット

空欄g … 社内LAN

となる。

設問2

cについて

番号10のルールは，向きがOUTであり，送信先ポート番号が80であることから，インターネット上のWebサーバへの要求パケットを通過させるための設定であるとわかる。社内LAN(プライベートIPアドレス)からインターネットへ向けての通信は，ファイアウォール2においてアドレス変換される。

変換後のグローバルIPアドレスは，ファイアウォール2のDMZ側インタフェースがもつグローバルIPアドレスである

220.1xx.2xx.4

なので，これを送信元IPアドレスとするパケットだけ許可すればよい。

dについて

番号15のルールは，社内LANのクライアントPCからWebサーバAを参照したときの応答パケットを通過させる設定である。したがって，送信元のIPアドレスとしてはWebサーバAのIPアドレス

210.2yy.1yy.100

を設定する。anywhereを設定すると，WebサーバA以外のホストからのパケットも通過させてしまうので，適切とはいえない。

jについて

社内LANに設置されているサーバはDHCPサーバ，メールサーバ，RADIUSサーバ，DNSサーバである。これらの中で認証サーバとしての役割をもつものは

RADIUSサーバ

である。RADIUS(Remote Authentication Dial In User Service)は，認証用のサーバを用い，一元的に認証管理を行う技術である。

設問3

hについて

NAPT(IPマスカレード)は，複数のプライベートIPアドレスを一つのグローバルIPアドレスに対応させるアドレス変換技術である。IPアドレスとポート番号を組み合わせて管理することで，複数のクライアントが一つのグローバルIPアドレスを共有することが可能になる。

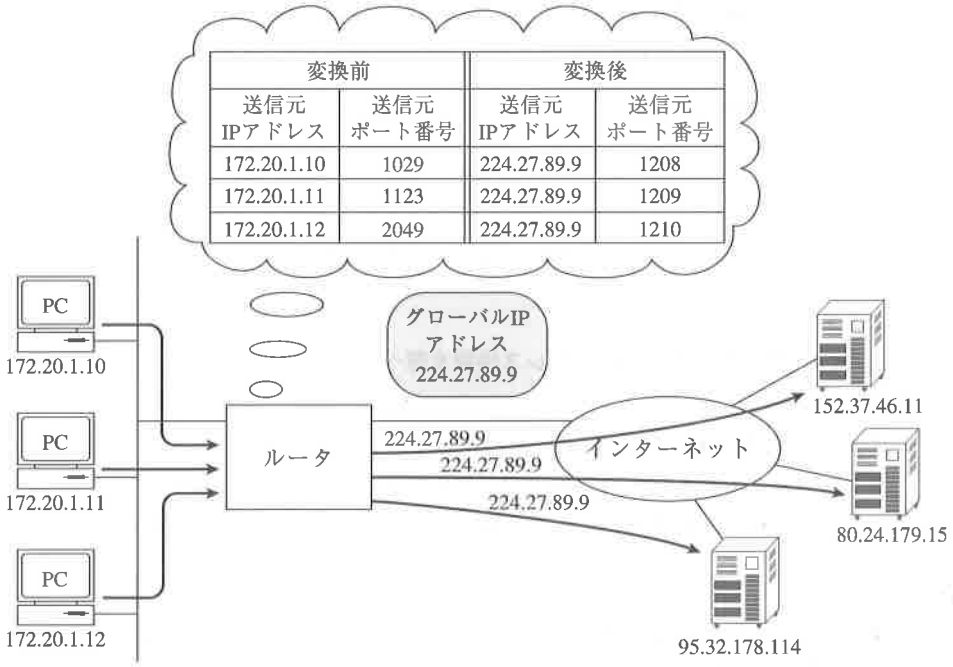


図3　NAPTのアドレス変換

NAPTでは，アドレス変換テーブルにポート番号とプライベートIPアドレスの組が登録されていないと，到着したパケットをどのプライベートIPアドレスに変換して良いのかを判断することができない。すなわち，いったん内側(プライベートIPアドレス側)から外側に向けての通信を行い，アドレス変換テーブルにポート番号とプライベートIPアドレスの組が登録された後でないと，外側からのパケットは内側のノードには届かない。

NAPTを利用すれば，インターネット側のホストが社内LANのホストのIPアドレスを知ることはできなくなる。よって，インターネット側から不正な接続開始を要求するパケットは，あて先が不正なものとして扱われ，社内LANに到着しなくなる。これによって，外部から不正に接続されて攻撃の対象となるリスクが減少する。

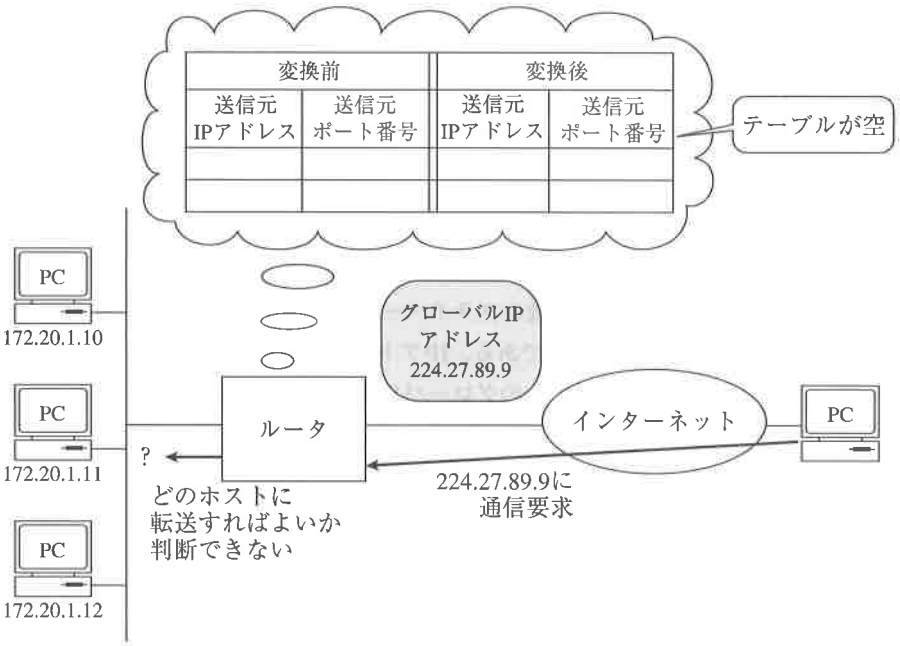


図4　外側からの接続時

以上をまとめて，解答としては，

社内LANのクライアントのアドレス情報を隠ぺいする

のように記述すればよい。

内部アドレスを隠ぺいし，外部からの不正接続を防ぐ

インターネットからの社内LANへ向けての接続を防ぐ

などのように，隠ぺいの結果として得られる効果について述べてもよいだろう。

kについて

前述のように，RADIUSサーバは，利用者IDやパスワードなどの認証情報を一元管理し，認証を行うサーバである。また，ログイン情報を記録することも可能である。本問のようにリモートアクセスサーバとともに用いるほか，IEEE802.1x認証(WPAを用いた無線LANアクセスポイントでの認証など)に用いることが多い。

本問では，リモートアクセスサーバを3台設置するとされている。このように複数に分散したアクセスサーバの認証情報(ログなど)をそのまま管理しようとすると，整合性保持などの管理負担が増大してしまうが，RADIUSサーバを設ければ，1台で認証情報を一元管理できるので，その負担を減らすことが期待できる。

設問4

eについて

TCPでは，送信時の順番どおりにパケットを受信できなくても元の並びに組み立て直せる，シーケンス制御を行っている。パケットを送った順を示すものがTCPヘッダのシーケンス番号である。

シーケンス番号の初期値は送信元と送信先との間でコネクションの開始時にランダムに決められるので，第三者がこれを知ることは困難である。つまり，シーケンス番号が妥当でないパケットが到着した場合，そのパケットは，第三者によって身元(送信元IPアドレス，送信元ポート番号)を偽ってインターネット上のサーバ(たとえばWebサーバAなど)になりすまし，不正に送りつけられたパケットである可能性がある。ステートフルインスペクション機能では，このようなパケットを検知し，アクセス制御を行う。

第三者が身元(送信元IPアドレス，送信元ポート番号)を偽って，すなわち，「なりすまして」不正にパケットを送りつけ，ファイアウォールを突破しようと試みる攻撃を

IPスプーフィング

という。

iについて

図2から，特定のホスト(220.2zz.1zz.40)からWebサーバ(220.1xx.2xx.1)に対して，ポート番号1～65535までの全ポートに対して繰り返し(順番に)接続を試みていることが読み取れる。このように，全ポートに対して接続が可能であるかどうかをスキャンし，攻撃口を探すことを

ポートスキャン

という。

攻撃者は，ポートスキャンによって接続可能なポートを見つけると，その後，攻撃を行い不正侵入し，権限奪取などを行う。ポートスキャン自体にはセキュリティ上の害は無いが，不正侵入の事前調査であると考えられるので，対策を行うことが好ましい。

問5

解答

TAC解答例

設問1		サイバー攻撃 1	ア		サイバー攻撃 2	イ	
		サイバー攻撃 3	オ		サイバー攻撃 4	カ	
設問2		a	プロキシサーバ		b	8080	
		c	DBサーバ		d	1521	
		e	メールサーバ1		f	25	
設問3	(1)	フ ァ イ ア ウ ォ ー ル に よ っ て D M Z に 到 達 す る					
		パ ケ ッ ト の 数 が 減 る た め					
	(2)	サイバー攻撃 （ 4 ）					

解説

設問1

選択肢に示された各攻撃の特徴をまとめると，次のようになる。

■DoS（サービス拒否）攻撃

サーバに対して大量の接続要求や処理要求，膨大なデータなどを送りつけ，サーバを過負荷状態に陥れることにより，サービスの提供を妨害する攻撃である。

■SQLインジェクション

入力データ中にSQL構文の一部を埋め込み，攻撃者が指示した任意のSQL文をデータベースサーバに実行させる攻撃である。入力データをそのまま利用してSQL文を組み立てているというプログラムの不備を利用する。

■ソーシャルエンジニアリング

技術的な攻撃手法を用いず，言葉巧みに人を欺いたり，職場のゴミ箱をあさったりして，秘密情報などを入手する手口である。

■トロイの木馬

有益なアプリケーションソフトウェア（ユーティリティソフト，ウイルス対策ソフト，ゲームなど）を装いつつ，裏では不正な処理を行う不正プログラムの一種である。コンピュータウイルスとは区別されることが多い。

■バッファオーバフロー攻撃

あらかじめ用意された入力バッファのサイズを超えるような大きなデータを入力し，入力バッファをあふれさせることによってプログラムの誤動作を誘引し，攻撃者が指定した処理を実行させる攻撃である。攻撃者が指定した処理は，攻撃対象のプログラムの動作権限で実行されるため，管理者権限で動作しているサーバプログラムが攻撃の対象となることが多い。

■ポートスキャン

サーバが提供中のサービスを調査する手口である。一般的には，すべてのポートに対して接続を試み，サーバからの反応があるポート(サービス)は提供中と判断する。実際に攻撃を行う前の準備段階として行われることが多い。

・サイバー攻撃1について

リクエストが大量に送られ，CPUとメモリの許容限度を超えてしまう旨の記述がある。サーバがこのような状態に陥ると，過負荷のためにサービスを正常に提供できなくなる。よって，サービスの提供を阻む，

DoS攻撃

が該当する。

・サイバー攻撃2について

DBサーバにアクセスするプログラムの不備を利用してデータベース上の情報に不正にアクセスしようとした旨の記述がある。DBサーバにアクセスするということは，SQL文を扱うことを意味する。よって，SQL文の一部を含む入力データを与え，不正なSQL文を実行する，

SQLインジェクション

が該当する。

・サイバー攻撃3について

プログラムが用意したメモリサイズを超えた入力を与えて，管理者権限を奪う旨の記述がある。ここでのプログラムが用意したメモリサイズとは，入力バッファのことであると考えられるので，あらかじめ用意された入力バッファのサイズを超える大きなデータを入力してプログラムの誤動作を誘引する，

バッファオーバフロー攻撃

が該当する。

・サイバー攻撃4について

使用可能なサービスを探した旨の記述がある。どのサービスが使えるのかは，実際にサーバプログラムに接続を試みて，サーバプログラムからの応答があるか否かを調査すればよい。よって，

ポートスキャン

が該当する。

設問2

表2の設定から，各項番がどのような通信を許可しているのかを整理すると，次のようになる。

表4　ファイアウォールが許可する通信

項番	通信内容
1	PC（内部LAN2）からメールサーバ2へメールを送信（ポート番号25） PC（内部LAN2）がメールサーバ2からメールを受信（ポート番号110）
2	PC（内部LAN2）からのDNSサーバ2へDNS問合せ
3	設問
4	社内からのメールを中継して社外メールサーバ（メールサーバ1）へ転送
5	社外からのメールを中継して社内メールサーバ（メールサーバ2）へ転送
6	設問
7	社外メールサーバ（メールサーバ1）が，社外へメールを送信
8	プロキシサーバがインターネット上のホストへ代理アクセス
9	社外（インターネット）からWebサーバへの通信
10	設問
11	インターネットからのDNSサーバ1へDNS問合せ
12	上記で許可した以外の通信はすべて禁止する（デフォルト禁止の設定）

a，bについて

項番3の通信は，送信元が内部LAN2（PC）となっているので，PC(社内)が行う通信を整理すればよい。PC(社内)と関連のあるサーバを表1から探すと，

① DNSサーバ2　　社内からの問合せに応答する
② メールサーバ2　　PCからのメール送受信要求を受け付ける
③ プロキシサーバ　　PCから社外へのWebアクセスを中継する

が，該当することがわかる。

①のDNSサーバ2との通信は項番2，②のメールサーバ2との通信は項番1で設定されているので，項番3で③の通信を許可するよう設定すればよい。本題文中の〔ファイアウォールの設定変更〕では，プロキシサーバが利用するポート番号について，「プロキシサーバへのアクセスは8080とする」と指定されているので，

送信元　内部LAN2
あて先　プロキシサーバ（空欄a）
サービス　8080（空欄b）

とすればよい。

c，dについて

項番6の通信は，送信元がWebサーバとなっているので，Webサーバと関連する通信を表1から探せばよい。サーバ名“Webサーバ”の行では，

① DBサーバにアクセス
② 取扱商品をインターネットに向けて紹介

となっている。取扱商品をインターネットに向けて紹介とは，インターネットからの問合せに応答することを意味するので，②のインターネットからの通信は項番9で設定されていると判断できる。よって，項番6では①の通信を許可するよう設定すればよい。本題文中の〔ファイアウォールの設定変更〕では，DBサーバが利用するポート番号について，「DBサーバへのアクセスは1521」と指定されているので，

送信元　Webサーバ
あて先　DBサーバ（空欄c）
サービス　1521（空欄d）

とすればよい。

e，fについて

項番10の通信は，送信元がインターネットとなっている。そこで，表1からインターネットから接続が行われる(インターネットが送信元となる)通信を整理すると，

① DNSサーバ1　　インターネットからの問合せに応答する
② Webサーバ　　インターネット向けに紹介する
③ メールサーバ1　　自社あてのメールをインターネットから受け取る

が，該当することがわかる

①のDNSサーバ1への問合せは項番11，②のWebサーバへの通信は項番9で設定されているので，項番10では③の通信を許可するよう設定すればよい。よって，

送信元　インターネット
あて先　メールサーバ1（空欄e）
サービス　25（空欄f）

とすればよい。

設問3

(1)

αとβの位置の違いに注目する。αの位置は，ファイアウォールの外側（バリアセグメント）であり，βの位置はファイアウォールの内側（DMZ）である。αの位置は，ファイアウォールの外側であるから，ファイアウォールによるフィルタリング（遮断）が一切されておらず，インターネットから送信されたすべてのパケットがこの位置を通過する。一方，βの位置は，ファイアウォールのフィルタリング機能によって，通過が許可されたパケットのみが通過する。したがって，IDSの設置位置をβの位置に変更したことによって警告メールが減少したのは，一定量の許可されないパケットがファイアウォールによってフィルタリングされたからと判断できる。解答は，この点を明確にし，

ファイアウォールによってDMZに到達するパケットの数が減るため

などと答えればよい。

(2)

警告メールが効果的に減少すると言うことは，該当の攻撃パケットが，ファイアウォール

によって遮断できるということを意味する。表3を見ると，IDSはサイバー攻撃1～4のいずれに対しても警告メールで通知する設定になっているので，ファイアウォールで遮断できる攻撃はどれかを考える。本問のファイアウォールは「あて先，送信元，サービスの組合せ」によって許可された通信のみを通過させ，許可されない通信を遮断するので，「あて先，送信元，サービスの組合せ」で遮断できるような攻撃を選べばよい。

サイバー攻撃4（ポートスキャン）では，使用可能なサービスを探すために，すべてのポート(サービス)に対して接続を試みる。許可されているサービスへの接続をファイアウォールで遮断することはできないが，許可されていないサービスへの接続はファイアウォールで遮断することが可能である。この結果，DMZに到着するパケット数が減少するので，IDSが検出する攻撃パケットの数も減少し，警告メールが減少すると考えられる。

以上より，警告メールが最も効果的に減少すると考えられるサイバー攻撃は，

サイバー攻撃4

である。

・サイバー攻撃1（DoS攻撃）について

この攻撃では，リクエストを大量にWebサーバに送りつける。正常なアクセスとの違いはリクエストの量だけであり，本問のファイアウォールでは正規のリクエストとの区別ができない。よって，DoS攻撃のパケットを遮断することはできず，IDSの警告メールを減らす効果は期待できない。

・サイバー攻撃2（SQLインジェクション）について

SQLインジェクションでは，入力データ中にSQL構文の一部を埋め込む。このため，SQLインジェクションの攻撃パケットは，パケットのデータ部(ペイロード部)を検査しなければ検出できない。本問のファイアウォールはパケットのデータ部(ペイロード部)を検査しないので，SQLインジェクションのパケットを遮断することはできず，IDSの警告メールを減らす効果は期待できない。

・サイバー攻撃3（バッファオーバフロー）について

バッファオーバフロー攻撃は，プログラムが用意したメモリサイズを超えるような長大なデータをプログラムに対して与える。このため，SQLインジェクションと同様に，パケットのデータ部（ペイロード部）を検査しなければ攻撃を検出することができず，本問のファイアウォールではバッファオーバフロー攻撃のパケットを遮断できない。したがって，αの位置とβの位置で攻撃パケット数に違いはなく，IDSの警告メールを減らす効果は期待できない。

TAC