

問040004解説

◆解答

設問1 a エ b イ c エ d エ

設問2 ウエ

◆解説

ファイアウォールのフィルタリング設定の問題である。

TCPとは

TCPはコネクション指向で、信頼性を提供するために再送信、パケットの順序制御、フロー制御や輻輳回避制御などネットワークの利用効率を高める数多くの機能をもっている。

コンピュータ上では複数のプログラムが同時に動作する。トランスポート層のプロトコルは、ポート番号を使って、通信しているプログラムを識別し、正しくデータを渡す処理を行う。通信の識別に、宛先IPアドレス、送信元IPアドレス、宛先ポート番号、送信元ポート番号、プロトコル番号を利用する。

ポート番号

アプリケーションに適切なデータを渡すためにポート番号を用いる。メール転送はポート番号25、HTTPのポート番号は80、FTPのポート番号は21、TELNETのポート番号は23、POP3のポート番号110などが決まっている。TCPはこのポート番号に従ってアプリケーションにデータを渡す。

SQLインジェクション攻撃

SQLインジェクションは、アプリケーションのセキュリティ上の不備を意図的に利用し、アプリケーションが想定しないSQL文を実行させることにより、データベースシステムを不正に操作する攻撃方法、また、その攻撃を可能とする脆弱性のことである。

設問1

フィルタリング設定ルールに関する問題である。

ファイアウォールAに関する設定

Webは、送信元が外部のインターネット上の任意からあて先Webサーバにポート番号80を指定して通信する。メール転送は、送信元が外部のインターネット上の任意からあて先メールサーバにポート番号25を指定して通信する。メール転送では、送信元がメールサーバからあて先が外部のインターネット上の任意にポート番号25を指定して通信する。aの答えはメールサーバで、求める答えはエとなる。bのポート番号は25で、求める答えはイとなる。

ファイアウォールBに関する設定

管理用PCはメールサーバを介して外部とのメールの送受信を行う。メールの送信はポート番号25を指定して通信するが、メールサーバからの受信はプロトコルPOP3を使用して、ポート番号110を指定して通信する。cのあて先の答えはメールサーバで、求める答えはエとなる。dのポート番号は110で、求める答えはエとなる。

設問2

アのWebサイトとやりとりするデータはインターネット上に公開されるものであり、盗聴は問題にならない。

イのインジェクションはアプリケーションの不備によって発生する問題であり、ファイアウォールのフィルタリング設定では防止できない。

ウのインターネットからDMZ内のサーバへの許可されていないポートでの接続は通信不可になるため防ぐことができる。

エのインターネットから社内LANへの不正アクセスはファイアウォールBのフィルタリングで防止できる。

オのメールによる社内ファイルの流出はメールの添付ファイルで送信されると、ファイアウォールのフィルタリングでは防止できない。

求める答えはウ、エとなる。