＜問 3＞　Web システムのセキュリティ診断

●設問 1

[試験センターによる解答例]

(1) N-IPS で遮断されていた PF 診断の通信が通過するから（27 字）
(2) ホワイトリストに診断 PC の IP アドレスを登録する。(25 字)
(3) a：(a)

＜解説＞

(1) N-IPS の脅威通信判定が有効な場合には、PF 診断において診断 PC が診断対象機器に対して行う通信の内容により、脅威と判定され、遮断される場合があるため、検出できない脆弱性が存在する可能性がある。一方、N-IPS の脅威通信判定を無効にすれば、こうしたことがなくなるため、より多くの脆弱性を検出する可能性がある。

(2) 表 1 の概要にあるように、N-IPS には、ホワイトリストに登録した IP アドレスからの通信は脅威ではないと判定する機能がある。したがって、診断 PC の IP アドレスをホワイトリストに登録すれば、N-IPS に通信を遮断されることなく PF 診断を実施することが可能である。

(3) 本番 Web サーバに対するインターネットから PF 診断は FW1、SSL アクセラレータ、N-IPS を経由することになる。FW1 では、インターネットから本番 Web サーバへの通信は必要なものだけを許可しているため、インターネットからの PF 診断に加え、図 1 中の接続点 (a) からの PF 診断も実施すべきである。そうすることにより、FW1 の有効性を検証するとともに、本番 Web サーバ自体の脆弱性を広く検出することも可能となる。

●設問 2

[試験センターによる解答例]

(1) b：診断用の利用者 ID（9 字）
(2) 変更する項目：日時
　変更する内容：診断時間を 0 時～8 時の間にする。(16 字)
(3) 機器：本番 DB サーバ
　変更後の設定：ホスト型 IPS のホワイトリスト設定に、診断 PC の IP アドレスを登録し、侵入検知設定を無効にする。(48 字)
(4) c：本番 DB サーバ
　d：DB 管理 PC
　e：許可

＜解説＞

(1) 問題文にあるように、Web 診断では、診断用の利用者 ID を作成し、それに診断用のポイントを付与した上で、P システムにログインして診断する。したがって、診断の終了後に削除する必要があるのは、診断用の利用者 ID である。

(2) 問題文の冒頭にあるように、P システムが受信する 1 日の時間帯別の通信量の比率は、0 時～8 時が 2%、8 時～16 時が 55%、16 時～24 時が 43%となっている。表 2 の診断計画では、診断を行う日時は 10 営業日の 9 時～17 時となっているため、診断によってサーバが異常停止した場合の影響が大きい。したがって、表 2 の項目で、これを最小化するために変更すべきなのは「日時」である。変更すべき内容としては、診断を実施する時間帯を、1 日の中で最も通信量が少ない 0 時～8 時の間にすることである。

(3) 診断 2 は本番 DB サーバに対する脆弱性診断である。表 1、図 2 にあるように、本番 DB サーバにはホスト型 IPS が導入されており、同 IPS のホワイトリスト設定や侵入検知設定による判定で通信が拒否されると、ポイントサービス部運用グループの執務室内にある警告灯が点灯する。また、図 2 の 1、2 より、同 IPS のホワイトリストには、現在、本番 Web サーバと DB 管理 PC の IP アドレスだけが登録されていること、侵入検知設定は無効にできることがわかる。したがって、診断 2 の実施にあたって警告灯が点灯しないよう設定を変更すべき機器は本番 DB サーバであり、変更内容は、同サーバのホスト型 IPS のホワイトリストに診断 PC の IP アドレスを追加登録するとともに、侵入検知設定を無効にすること

である。

(4) 表 1 の FW2 の概要にあるように、FW2 では、管理 PC セグメントから本番 Web サーバ、本番 DB サーバ、ステージング Web サーバ及びステージング DB サーバへの通信を許可しているが、最近配属された担当者が Web 管理 PC から本番 DB サーバにログインを試みた結果、同サーバのホスト型 IPS によって通信が拒否され、警告灯が点灯することとなった。図 1 にあるように、本来、管理 PC セグメントから本番 DB サーバに通信する必要があるのは DB 管理 PC のみである。したがって、再発防止策としては、本番 DB サーバ宛ての通信については、DB 管理 PC からの通信だけを許可するように FW2 のルールを修正するのが有効である。ただし、これを行うと、図 1 の（e）に診断 PC を接続した場合には、診断 PC から本番 DB サーバへの通信が FW2 によって遮断されてしまうことになる。そのため、運用グループは、診断 PC の接続ポイントを図 1 の（e）から（d）に変更するよう提案したのである。