次の問1は必須問題です。必ず解答してください。

問1　ネットワークや Web アプリケーションプログラムのセキュリティに関する次の記述を読んで，設問1～4に答えよ。

X社は，中堅の機械部品メーカである。X社では，部品製造に関わる特許情報や顧客情報を取り扱うので，社内のネットワークセキュリティを強化している。社内のネットワークの内部セグメントには，内部メールサーバ，内部 Web サーバ，ファイルサーバなど社内業務を支援する各種サーバが配置されている。また，DMZ には，インターネット向けのメール転送サーバ，DNS サーバ，Web サーバ，プロキシサーバが配置されている。Web サーバでは，製品情報や特定顧客向けの部品情報の検索システムを社外に提供しており，内部 Web サーバやファイルサーバでは，特許情報や顧客情報の検索システムを社内に提供している。X社のネットワーク構成を図1に示す。

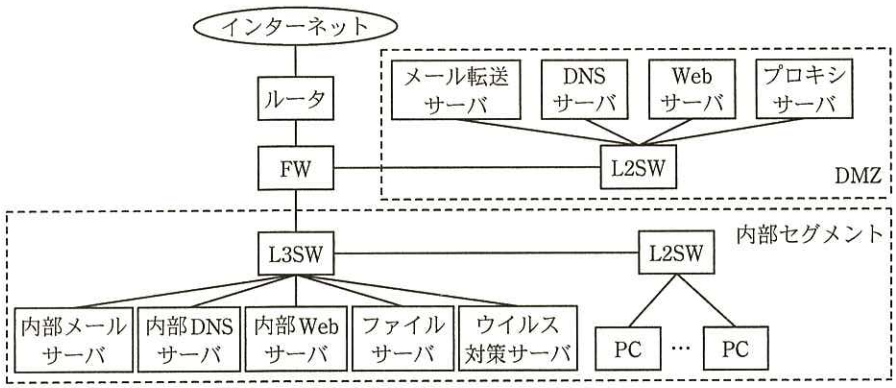

図1　X社のネットワーク構成

先日，同業他社の社外向け Web サイトが外部からの攻撃を受けるというセキュリティインシデントが発生したことを聞いた情報システム部の Y 部長は，特に FW に関するネットワークセキュリティの強化を検討するように部下の Z さんに指示した。

X社の社内ネットワークのセキュリティ要件を図2に示す。

1. 共通事項
  1.1 社内の通信機器やサーバがインターネットと通信する場合には，FW などの装置を用いてアクセス制御を行うこと。
  1.2 業務上必要がない通信は全て禁止すること。
  1.3 インターネットに公開する社内のサーバは必要最小限にとどめること。
2. Web
  2.1 社内の PC から社外 Web サイトへの HTTP 通信（HTTPS を含む。以下同じ）は，プロキシサーバ経由で行うこと。
  2.2 社外から社内への HTTP 通信は，インターネットから Web サーバへの HTTP 通信だけを許可すること。
  2.3 Web アプリケーションプログラムの脆弱性を悪用した攻撃を防ぐために，インターネットから Web サーバにアクセスする通信は，あらかじめ定められた一連の手続の HTTP 通信だけを許可すること。
3. 電子メール
  3.1 社内の PC 間のメール通信は，内部メールサーバを介して行うこと。
  3.2 内部セグメントと DMZ の間のメール通信は，内部メールサーバとメール転送サーバの間だけを許可すること。
  3.3 社内と社外の間のメール通信は，メール転送サーバとインターネットの間だけを許可すること。
4. DNS
（以下省略）

図２　X社の社内ネットワークのセキュリティ要件（抜粋）

Z さんは，①FW による IP アドレスやポート番号を用いたパケットフィルタリングだけでは外部からの攻撃を十分に防ぐことができないと考えた。そこで，より高度なセキュリティ製品の追加導入を検討するために，IDS，IPS や WAF の基本的な機能について調査した。調査の結果，IDS は，X 社の外部からの［ a ］ことができ，IPS は，X 社の外部からの［ b ］ことができ，一方，WAF は，［ c ］ことができるということが分かった。

この結果から，Z さんは，次の二つの案を考えた。

案 1：社内ネットワークのルータと FW の間にネットワーク型の IPS を導入する。

案 2：セキュリティ強化の対象とするサーバに WAF を導入する。

今回，［ d ］を目的とする場合には案 1 を，［ e ］を目的とする場合には案 2 を選択することがそれぞれ有効であると分かった。

特に案 2 の WAF は，ブラックリストや②ホワイトリストの情報を有効に活用することで，社内ネットワークのセキュリティ要件 2.3 を満たすことができる。

Z さんは，それぞれの案について，費用面や運用面での課題の比較検討も行い，結果を取りまとめて Y 部長に報告した。これを受けて Y 部長は，案 2 を採用することを決め，具体的な実施策を検討するように Z さんに指示した。

設問 1　本文中の下線①において，FW では防げない攻撃を解答群の中から全て選び，記号で答えよ。

解答群

ア　DNS サーバを狙った，外部からの不正アクセス攻撃

イ　Web サーバの Web アプリケーションプログラムの脆弱性を悪用した攻撃

ウ　内部 Web サーバを狙った，外部からの不正アクセス攻撃

エ　ファイルサーバを狙った，外部からの不正アクセス攻撃

オ　プロキシサーバを狙った，外部からのポートスキャンを悪用した攻撃

設問 2　本文中の［　a　］～［　c　］に入れる最も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　IP パケットの中身を暗号化して盗聴や改ざんを防止する

イ　IP パケットの中身を調べて不正な挙動を検出し遮断する

ウ　IP パケットの中身を調べて不正な挙動を検出する

エ　Web アプリケーションプログラムとのやり取りに特化した監視や防御をする

オ　Web アプリケーションプログラムとのやり取りを暗号化して盗聴や改ざんを防止する

カ　電子メールに対してウイルスチェックを行う

設問 3　本文中の［　d　］，［　e　］に入れる最も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　PC に対するウイルス感染チェック

イ　Web サーバの Web アプリケーションプログラムの脆弱性を悪用した攻撃の検出や防御

ウ　外部からの不正アクセス攻撃の検出や防御を X 社の社内ネットワーク全体に対して行うこと

エ　内部からの不正アクセス攻撃の検出や防御を X 社の社内ネットワーク全体に対して行うこと

オ　内部メールサーバに対する不正アクセス攻撃の検出や防御

設問 4　本文中の下線②のホワイトリストに，どのような通信パターンを登録する必要があるか。図 2 中の字句を用いて 30 字以内で述べよ。