マルウェア対策

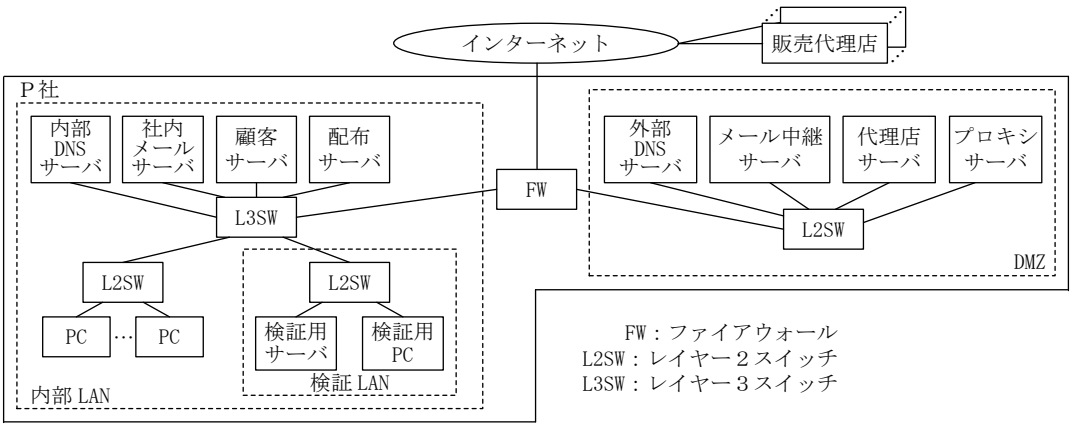
問 6 Check □ □ □ 【2022年秋期 応用情報 問1】

マルウェアへの対応策に関する次の記述を読んで，設問に答えよ。

P社は，従業員数 400 名の IT 関連製品の卸売会社であり，300 社の販売代理店をもっている。P社では，販売代理店向けに，インターネット経由で商品情報の提供，見積書の作成を行う代理店サーバを運用している。また，従業員向けに，代理店ごとの卸価格や担当者の情報を管理する顧客サーバを運用している。代理店サーバ及び顧客サーバには，HTTP Over TLS でアクセスする。

P社のネットワークの運用及び情報セキュリティインシデント対応は，情報システム部（以下，システム部という）の運用グループが行っている。

P社のネットワーク構成を図１に示す。



注記１ 配布サーバは，PC にセキュリティパッチなどを配布するサーバである。

注記２ 検証 LAN は，サーバ及び PC の動作検証などを行うための LAN である。

図１ P社のネットワーク構成

〔セキュリティ対策の現状〕

P社では，複数のサーバ，PC 及びネットワーク機器を運用しており，それらには次のセキュリティ対策を実施している。

- [a] では，インターネットと DMZ 間及び内部 LAN と DMZ 間で業務に必要な通信だけを許可し，通信ログ及び遮断ログを取得する。
- [b] では，SPF（Sender Policy Framework）機能によって送信元ドメイン認証を行い，送信元メールアドレスがなりすまされた電子メール（以下，電子メールをメールという）を隔離する。
- 外部 DNS サーバでは，DMZ のゾーン情報の管理のほかに，キャッシュサーバの機能を稼働させており，外部 DNS サーバを①DDoS の踏み台とする攻撃への対策を行う。
- P社からインターネット上の Web サーバへのアクセスは，DMZ のプロキシサーバを経由し，プロキシサーバでは，通信ログを取得する。

・PC 及びサーバで稼働するマルウェア対策ソフトは，毎日，決められた時刻にベンダーの Web サイトをチェックし，マルウェア定義ファイルが新たに登録されている場合は，ダウンロードして更新する。
・システム部の担当者は，毎日，ベンダーの Web サイトをチェックし，OS のセキュリティパッチやアップデート版の有無を確認する。最新版が更新されている場合は，ダウンロードして検証 LAN で動作確認を１週間程度行う。動作に問題がなければ，PC 向けのものは［ c ］に登録し，サーバ向けのものは，休日に担当者が各サーバに対して更新作業を行う。
・PC は，電源投入時に［ c ］にアクセスし，更新が必要な新しい版が登録されている場合は，ダウンロードして更新処理を行う。
・FW 及びプロキシサーバのログの検査は，担当者が週に１回実施する。

〔マルウェアＸの調査〕

ある日，システム部のＱ課長は，マルウェアＸの被害が社外で多発していることを知り，Ｒ主任にマルウェアＸの調査を指示した。Ｒ主任による調査結果を次に示す。

(1) 攻撃者は，不正なマクロを含む文書ファイル（以下，マクロ付き文書ファイルＡという）をメールに添付して送信する。
(2) 受信者が，添付されたマクロ付き文書ファイルＡを開きマクロを実行させると，マルウェアへの指令や不正アクセスの制御を行うインターネット上の C&C サーバと通信が行われ，マルウェアＸの本体がダウンロードされる。
(3) PC に侵入したマルウェアＸは，内部ネットワークの探索，情報の窃取，窃取した情報の C&C サーバへの送信及び感染拡大を，次の(a)～(d)の手順で試みる。
　(a) ②PC が接続するセグメント及び社内の他のセグメントの全てのホストアドレス宛てに，宛先アドレスを変えながら ICMP エコー要求パケットを送信し，連続してホストの情報を取得する。
　(b) ③(a)によって情報を取得できたホストに対して，攻撃対象のポート番号をセットした TCP の SYN パケットを送信し，応答内容を確認する。
　(c) (b)で SYN/ACK の応答があった場合，指定したポート番号のサービスの脆弱(ぜいじゃく)性を悪用して個人情報や秘密情報などを窃取し，C&C サーバに送信する。
　(d) 侵入した PC に保存されている過去にやり取りされたメールを悪用し，当該 PC 上でマクロ付き文書ファイルＡを添付した返信メールを作成し，このメールを取引先などに送信して感染拡大を試みる。

Ｒ主任が調査結果をＱ課長に報告したときの，２人の会話を次に示す。

Ｑ課長：マルウェアＸに対して，現在の対策で十分だろうか。
Ｒ主任：十分ではないと考えます。文書ファイルに組み込まれたマクロは，容易に処理内容が分析できない構造になっており，マルウェア対策ソフトでは発見できない場合があります。また，④マルウェアＸに感染した社外の PC から送られてきたメールは，SPF 機能ではなりすましが発見できません。
Ｑ課長：それでは，マルウェアＸに対する有効な対策を考えてくれないか。
Ｒ主任：分かりました。セキュリティサービス会社のＳ社に相談してみます。

マルウェア対策

〔マルウェアＸへの対応策〕

Ｒ主任は，現在のセキュリティ対策の内容をＳ社に説明し，マルウェアＸに対する対応策の提案を求めた。Ｓ社から，セキュリティパッチの適用やログの検査が迅速に行われていないという問題が指摘され，マルウェアＸ侵入の早期発見，侵入後の活動の抑止及び被害内容の把握を目的として，EDR（Endpoint Detection and Response）システム（以下，EDR という）の導入を提案された。

Ｓ社が提案した EDR の構成と機能概要を次に示す。

・EDR は，管理サーバ，及び PC に導入するエージェントから構成される。
・管理サーバは，エージェントの設定，エージェントから受信したログの保存，分析及び分析結果の可視化などの機能をもつ。
・エージェントは，次の(ⅰ)，(ⅱ)の処理を行うことができる。
(ⅰ) PC で実行されたコマンド，通信内容，ファイル操作などのイベントのログを管理サーバに送信する。
(ⅱ) PC のプロセスを監視し，あらかじめ設定した条件に合致した動作が行われたことを検知した場合に，設定した対応策を実施する。例えば，EDR は，(a)～(c)に示した⑤マルウェアＸの活動を検知した場合に，⑥内部ネットワークの探索を防ぐなどの緊急措置を PC に対して実施することができる。

Ｒ主任は，Ｓ社の提案を基に，マルウェアＸの侵入時の対応策をまとめ，Ｑ課長に EDR の導入を提案した。提案内容は承認され，EDR の導入が決定した。

設問１　〔セキュリティ対策の現状〕について答えよ。

(1) 本文中の［ a ］～［ c ］に入れる適切な機器を，解答群の中から選び記号で答えよ。

解答群

ア　FW	イ　L2SW	ウ　L3SW
エ　外部 DNS サーバ	オ　検証用サーバ	カ　社内メールサーバ
キ　内部 DNS サーバ	ク　配布サーバ	ケ　メール中継サーバ

(2) 本文中の下線①の攻撃名を，解答群の中から選び記号で答えよ。

解答群

ア　DNS リフレクション攻撃　　イ　セッションハイジャック攻撃
ウ　メール不正中継攻撃

設問２　〔マルウェアＸの調査〕について答えよ。

(1) 本文中の下線②の処理によって取得できる情報を，20 字以内で答えよ。

(2) 本文中の下線③の処理を行う目的を，解答群の中から選び記号で答えよ。

解答群

ア　DoS 攻撃を行うため
イ　稼働中の OS のバージョンを知るため
ウ　攻撃対象のサービスの稼働状態を知るため
エ　ホストの稼働状態を知るため

(3) 本文中の下線④について，発見できない理由として最も適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　送信者のドメインが詐称されたものでないから
イ　添付ファイルが暗号化されているので，チェックできないから
ウ　メールに付与された署名が正規のドメインで生成されたものだから
エ　メール本文に不審な箇所がないから

設問３　〔マルウェアＸへの対応策〕について答えよ。

(1) 本文中の下線⑤について，どのような事象を検知した場合に，マルウェアＸの侵入を疑うことができるのかを，25 字以内で答えよ。

(2) 本文中の下線⑥について，緊急措置の内容を 25 字以内で答えよ。

(3) EDR 導入後にマルウェアＸの被害が発生したとき，被害内容を早期に明らかにするために実施すべきことは何か。本文中の字句を用いて 20 字以内で答えよ。

マルウェア対策