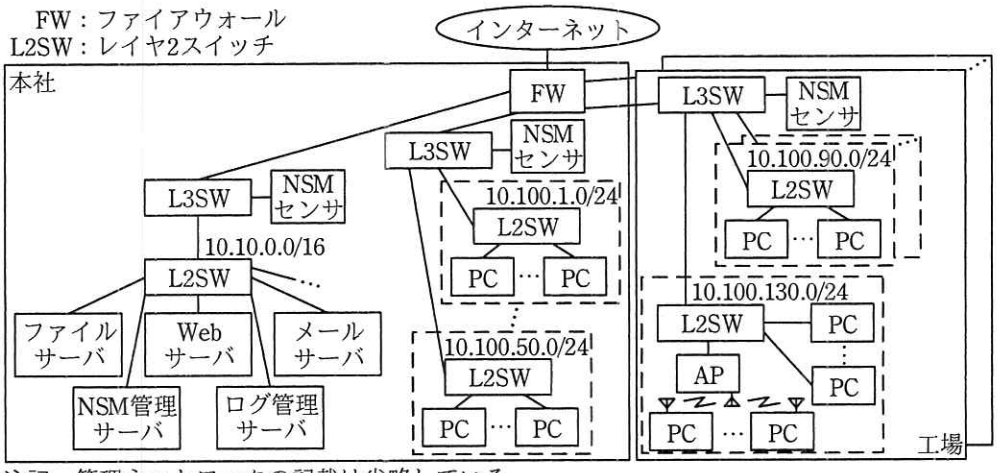
問２　セキュリティインシデント対応に関する次の記述を読んで，設問１～４に答えよ。

G 社は，従業員数 1,200 名の製造業者であり，本社と四つの工場がある。工場には，無線 LAN アクセスポイント（以下，AP という）を導入している。本社及び各工場には，レイヤ３スイッチ（以下，L3SW という）及び，ネットワークセキュリティモニタリング（以下，NSM という）のセンサが設置されている。NSM センサには，シグネチャ型の IDS 機能に加えて，ネットワークフロー情報（以下，NF 情報という）を記録する機能がある。NF 情報は，流れている全てのパケットについて，ヘッダ情報を参照し，“コネクション開始日時，送信元 IP アドレス，宛先 IP アドレス，送信元ポート，宛先ポート，プロトコル，コネクションステータス，コネクション時間，送信バイト数，受信バイト数”をコネクション単位でレコード化したものである。NF 情報は，NSM センサから管理ネットワークを通じて NSM 管理サーバに送信され，統合管理されている。G 社のネットワーク構成を図１に示す。



注記　管理ネットワークの記載は省略している。

図１　G 社のネットワーク構成

L3SW には，スイッチの特定の物理ポートを流れるパケットを，ミラーポートという別の物理ポートにミラーリングする機能があり，ネットワーク障害発生時にパケットを取得する用途でも使われている。L3SW では，FW に接続している 1G ビット／秒（以下，ビット／秒を bps という）の物理ポートを流れるインとアウトのパケットを，NSM センサに接続している 10Gbps のミラーポートにミラーリングしている。

ミラーポートに流れる通信量は，全二重 1Gbps の 1 ポートの送受信をミラーリングする場合，最大 [a] bps となる。L3SW 及び L2SW は，VLAN をサポートしている機器であるが，G 社では VLAN の設定はしていない。VLAN を設定する場合，L3SW では，IEEE 802.1Q の [b] を付与した状態でミラーリングできるので，障害が発生している VLAN を識別できる。ミラーポートを使用せずにパケットを取得する方法として，ネットワーク [c] を使用する方法もある。

〔セキュリティインシデントの発生〕

ある日，セキュリティ管理部の J 主任に NSM 管理サーバからアラートメールが届いた。J 主任は，部下の M 君とともに調査を開始した。NSM 管理サーバのダッシュボード画面を確認したところ，IDS 機能のアラートは発生していなかったが，通信量が普段よりも 2 倍以上増えていたのでアラートメールが送られたことが分かった。そこで，NSM 管理サーバを使って，通信量が増えている原因を調べることにした。まず，直近 1 時間のコネクション件数を表示してみた。表示内容を図 2 に示す。

送信元 IP アドレス別の件数（Top10）

送信元 IP アドレス	件数
10.100.130.1	40,435,457
10.100.1.2	1,545,454
10.100.3.2	1,435,094
10.100.5.10	1,420,195
10.100.90.121	1,417,872
10.100.100.2	1,401,370
⋮	⋮

宛先 IP アドレス別の件数（Top10）

宛先 IP アドレス	件数
10.10.10.10	5,684,129
10.10.10.20	4,396,545
10.10.10.50	3,834,903
10.10.20.30	3,112,935
10.10.20.20	2,487,456
10.10.10.90	1,843,623
⋮	⋮

宛先ポート別の件数（Top10）

宛先ポート	件数
445/TCP	46,862,012
80/TCP	8,540,743
443/TCP	3,541,089
587/TCP	442,530
53/UDP	423,668
123/UDP	405,759
⋮	⋮

TCP ステータス別の件数（Top10）

ステータス	件数
SYN に対して応答なし	40,873,561
SYN/FIN で正常終了	11,353,579
SYN なし ACK だけ	845,396
宛先からの RST で終了	34,675
送信元からの RST で終了	13,961
⋮	⋮

図 2　NSM 管理サーバのダッシュボード画面（直近 1 時間のコネクション件数）

宛先ポート別の件数で，445/TCP のコネクション件数が普段と比べて非常に多かった。J 主任は，セキュリティ機関から，ワーム V に関する注意喚起を受け取っていた

ことを思い出した。ワーム V に関する注意喚起を図 3 に示す。

・ワーム V は，Windows の脆弱性を悪用し，ファイル共有で使われる 445/TCP のポートを経由して感染を広めるものであり，複数の組織でネットワークに障害が発生している。
・ワーム V は，次の 2 種類の IP アドレス範囲に対して，並行して 445/TCP のポートをスキャンし，①正常な応答がある場合に，脆弱性を悪用して感染を試みる。
(a) 感染した PC と同一セグメントの範囲
(b) 1.1.1.1 から 223.255.255.255 の範囲

スキャンでは，各 IP アドレスに 1 パケットずつ接続要求を送信する。(a)のスキャンでは，IP アドレス範囲の最後までスキャンが完了した場合，5 分間待機した後，IP アドレス範囲の先頭からスキャンを繰り返す。(b)のスキャンは，IP アドレス範囲の最後までスキャンが完了した場合，スキャンを終了する。

図 3　ワーム V に関する注意喚起

J 主任はワーム V が原因であると仮定して分析を進めた。送信元 IP アドレス別の件数では，10.100.130.1 の件数が普段と比較して非常に多かった。宛先 IP アドレス別の件数では，ファイルサーバや Web サーバなどが件数の上位になっており，普段と比べて大きな違いはなかった。②ワーム V が行うスキャンは，宛先 IP アドレス別の件数の上位に登場していない。TCP ステータス別の件数では，“SYN に対して応答なし”が多くなっているが，これはワーム V のスキャンに対して，宛先 IP アドレスから応答がないことを示していると考えた。ここまでの調査結果から，10.100.130.1 の IP アドレスをもつ機器がワーム V に感染している可能性があると判断し，ネットワークの停止をアナウンスして，L2SW で，10.100.130.1 の機器がつながっている物理ポートをシャットダウンした。

〔無線 LAN セグメントの調査〕

10.100.130.1 は，ルータとして動作している AP に割り当てた IP アドレスであることが分かった。AP では NAPT で IP アドレスの変換をして PC と接続していることから，AP に接続している PC がワーム V に感染している可能性があると判断した。これらの PC の IP アドレスは AP の DHCP サーバ機能で設定していることから，AP の通信ログ及び DHCP サーバ機能のログ（以下，DHCP サーバログという）を調査することにした。

DHCP サーバ機能では，IP アドレスのリース期間を 1 時間に設定しており，プー

ルしている IP アドレス範囲から適宜リースする。AP での通信ログのうち宛先 IP アドレスが G 社の利用していない IP アドレスであり，かつ，宛先ポートが 445/TCP のものを表 1 に示す。表 2 に 10 月 28 日の AP の DHCP サーバログを示す。M 君は，表 1 と表 2 を基に，445/TCP のポートをスキャンしている PC を特定した。

表 1　AP の通信ログ

日時	NAPT 変換前 IP アドレス	NAPT 変換後 IP アドレス	宛先 IP アドレス	宛先ポート
10/28 14:25:02 [1]	192.168.0.32	10.100.130.1	1.1.1.1	445
⋮	⋮	⋮	⋮	⋮
10/28 14:26:45 [1]	192.168.0.8	10.100.130.1	1.1.1.1	445
⋮	⋮	⋮	⋮	⋮
10/28 14:27:18 [1]	192.168.0.44	10.100.130.1	1.1.1.1	445
⋮	⋮	⋮	⋮	⋮
10/28 16:51:50 [1]	192.168.0.12	10.100.130.1	1.1.1.1	445
⋮	⋮	⋮	⋮	⋮
10/28 17:31:22	192.168.0.44	10.100.130.1	1.100.2.45	445
10/28 17:31:23	192.168.0.32	10.100.130.1	1.100.1.37	445
10/28 17:31:25	192.168.0.12	10.100.130.1	1.50.2.30	445
10/28 17:31:25	192.168.0.8	10.100.130.1	1.100.1.201	445

注記　省略された期間のログにおいて，NAPT 変換前 IP アドレスは，本表に記載されている IP アドレスだけが記録されている。

注 [1]　それぞれの NAPT 変換前 IP アドレスが最初に記録された日時である。

表 2　AP の DHCP サーバログ

日時	IP アドレス	MAC アドレス	ホスト名
10/28 10:45:38	192.168.0.8	X	PC101
10/28 10:46:12	192.168.0.12	J	PC204
10/28 10:46:49	192.168.0.32	P	PC301
10/28 10:46:53	192.168.0.21	U	PC145
10/28 10:47:11	192.168.0.44	T	PC277
10/28 10:48:20	192.168.0.4	H	PC132
10/28 10:49:03	192.168.0.112	S	PC105
10/28 10:49:47	192.168.0.55	R	PC298
10/28 14:24:50	192.168.0.32	M	PC321
10/28 16:51:13	192.168.0.44	G	PC133
10/28 16:51:42	192.168.0.12	X	PC101
10/28 16:52:37	192.168.0.32	N	PC340
10/28 16:54:29	192.168.0.8	P	PC301
10/28 22:53:45	192.168.0.8	Z	PC333
10/28 22:55:04	192.168.0.21	U	PC145
10/28 22:55:32	192.168.0.55	R	PC298
10/28 22:56:33	192.168.0.4	H	PC132
10/28 22:57:58	192.168.0.44	T	PC277
10/28 22:58:17	192.168.0.12	K	PC104

注記 1　IP アドレスのリースは記録されているが，IP アドレスのリリースは記録されていない。

注記 2　本表では MAC アドレスを英字 1 字で表記している。

〔セキュリティインシデントの再発防止策〕

M 君は，無線 LAN のパケットをキャプチャしたところ，6 台の PC が，[d] リクエストをブロードキャストで送信して，同一セグメント内の PC を探索していることを確認した。

M 君は，無線 LAN に接続している PC のうち 6 台がワーム V に感染している可能性を J 主任に報告した。J 主任は，感染有無を確認するよう指示した。セキュリティ機関からは，ワーム V のインディケータ情報が [e] 形式で提供されていた。そこで M 君がそのインディケータ情報を使ってファイルを検索して，感染の有無を確認したところ，6 台ともワーム V に感染していることが分かった。

通信ログ及びワーム V のファイルの作成日時から，最初に感染したのは，IP アドレスが 192.168.0.32 の PC であり，この PC から他の PC へ感染が広がったことが分かった。この PC は，社外に持ち出して公衆無線 LAN に接続した際，セキュリティ修正プログラムが未適用で，かつ，マルウェア対策ソフトのマルウェア定義ファイルが更新されていない状態だったので，ワーム V に感染したと考えられた。G 社では，PC を社外に持ち出した際の情報漏えい対策を行っていたが，社外でワームに感染した PC を持ち帰るリスクは想定していなかった。

J 主任は，セキュリティインシデントの初動対応として，必要な措置を実施した。また，ワーム V に感染した PC が G 社のネットワーク内に新たに持ち込まれる可能性があるので，NSM センサの IDS 機能のシグネチャを更新して，ワーム V による感染活動のパケットを監視することにした。

次に，再発防止策として，無線 LAN には，社外に持ち出した PC を接続することが多いので，③PC を持ち帰った際に接続可否を判断するためにチェックを行うことにした。さらに，有線 LAN では，④同じ L2SW に接続された PC 同士のワーム感染を防ぐ対策を実施することにした。

J 主任は，調査結果を上司に報告し，再発防止策を実施して，セキュリティインシデントの対応を完了した。

設問1　本文中の［　a　］～［　e　］に入る語句を解答群から選び，記号で答えよ。

解答群

ア　10G	イ　1G	ウ　2G
エ　ARP	オ　CVE	カ　ECHO
キ　HTTP	ク　NOC	ケ　RF タグ
コ　STIX	サ　TAXII	シ　TLP
ス　VLAN タグ	セ　タップ	ソ　ロードバランサ

設問2　〔セキュリティインシデントの発生〕について，(1)，(2) に答えよ。

(1)　図 3 中の下線①について，どのような TCP フラグの組合せの応答か。8 字以内で答えよ。

(2)　本文中の下線②について，ワーム V が行うスキャンの特徴を踏まえて，図 3 中の(a)及び(b)のスキャンが宛先 IP アドレス別の件数の上位に登場しない理由を，それぞれ 25 字以内で述べよ。

設問3　〔無線 LAN セグメントの調査〕について，(1)，(2) に答えよ。

(1)　AP の通信ログと DHCP サーバログを調査して，ワーム V に感染したと判断すべき PC を全て答えよ。

なお，解答に当たっては，答案用紙に記載した表 2 中の各 PC のホスト名を○印で囲んで示せ。

(2)　感染した PC による通信を調べてみると，DHCP によって IP アドレスが変わったので，感染した複数の PC が同じ送信元 IP アドレスを使っている場合がある。感染した複数の PC によって使われた送信元 IP アドレスを解答群から全て選び，記号で答えよ。

解答群

ア　192.168.0.4	イ　192.168.0.8	ウ　192.168.0.12
エ　192.168.0.21	オ　192.168.0.32	カ　192.168.0.44
キ　192.168.0.55	ク　192.168.0.112	

設問4　〔セキュリティインシデントの再発防止策〕について，(1)，(2) に答えよ。

(1)　本文中の下線③について，チェックすべき内容を二つ挙げ，それぞれ 30 字以内で述べよ。

(2)　本文中の下線④を実現するために行う設定を 25 字以内で述べよ。