SC

平成30年度　秋期
情報処理安全確保支援士試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問3
選択方法	2問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ソフトウェア開発に関する次の記述を読んで，設問1～3に答えよ。

U社は，IoT機器の開発を行う，従業員数400名の企業である。IoT機器のソフトウェアの開発にはC/C++言語を使っている。IoT機器に搭載するOSには，Linuxを利用してきたが，今後はLinux以外も利用する予定である。これまで製品に大きなトラブルはなかったが，2020年東京オリンピック・パラリンピックに向けてIoT機器に関するセキュリティリスクが高まると経営層が判断し，開発におけるセキュリティ対策を強化することになった。そこで，開発部のL部長とX主任がセキュリティ対策技術を調査した。

〔メモリ破壊攻撃の概要〕

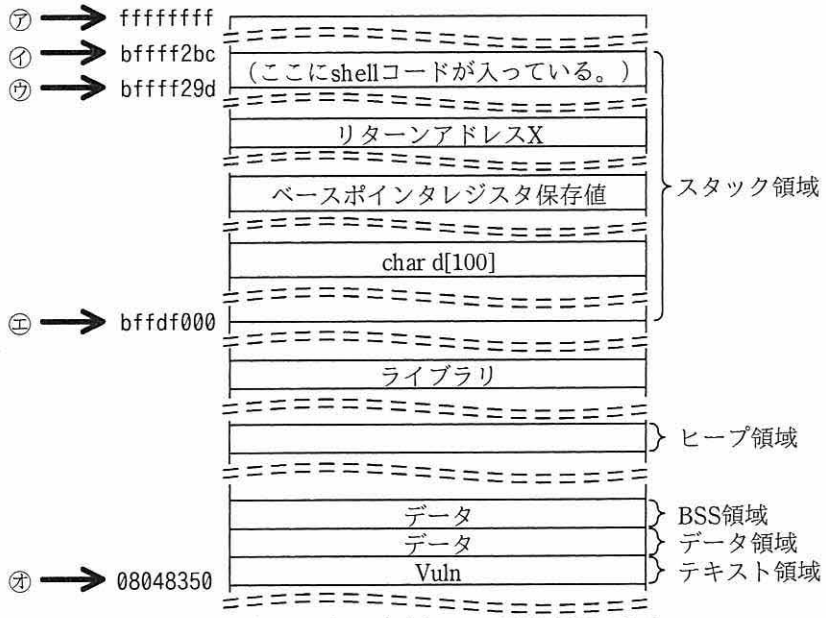
メモリ破壊脆弱(ぜい)性は，プログラム実行時に，メモリ上にある制御情報を書き換えることによって，実行制御を奪うなどのメモリ破壊攻撃に悪用される。メモリ破壊脆弱性の一種にバッファオーバフロー脆弱性がある。

例えば，図1に示すプログラムVulnがあったとする。Vulnは，スタックバッファオーバフロー脆弱性の学習用に作成した，32ビット版Linuxで実行可能なプログラムである。図2はVuln内の関数fooが呼び出された後のメモリマップである。プログラム実行時に，変数bが指し示すデータが不正な場合，そのデータによって，［　a　］が［　あ　］に書き換えられると，関数fooの終了時にshellコードへ処理が遷移する。しかし，①このような遷移があっても，データ実行防止機能（以下，DEPという）が機能していると，攻撃は成功しない。

攻撃者が，DEPを回避するため，図2中のshellコードへ処理を遷移させる代わりに，［　b　］中の実行可能なコードや［　c　］領域にマップされているVulnの断片コードを利用するケースがある。例えば，攻撃の際，［　a　］を［　b　］関数の先頭アドレスで書き換えて，攻撃者の意図した［　b　］関数を呼び出す［　d　］攻撃もある。

```
      (省略)
 1:   int main(int argc, char *argv[]) {
 2:     char *a, *x;
        (省略, argvに応じてサイズを確保する。)
        (省略, ここでa, xがポイントする領域にargvからデータをコピーする。)
 3:     foo(a, x);
        (省略, ここでその他の必要な処理をする。)
 4:   }
 5:   int foo(char *b, char *c) {
 6:     char d[100];
        (省略)
 7:     strcpy(d, b);
 8:     if (d[0] == 0) {
 9:       err_out(c);
          (省略)
10:     }
        (省略)
11:     return 0;
12:   }
13:   int err_out(char *errmsg) {
14:     char s1[100];
15:     int i=0;
        (省略)
16:     while ((s1[i++] = *errmsg++) != '¥0');
17:     fprintf(stderr, "Error : %s ¥n", s1);
        (省略)
18:     return 0;
19:   }
```

図1　スタックバッファオーバフロー脆弱性のあるプログラム Vuln



注記　メモリアドレスは4バイトの16進数表記である。

図2　関数 foo が呼び出された後のメモリマップ

〔メモリ破壊攻撃に対する対策技術〕

現在，メモリ破壊攻撃に対する対策技術（以下，M 対策技術という）が普及している。X 主任は，DEP を含めた代表的な M 対策技術を調査し，表 1 にまとめた。

表 1　M 対策技術の概要

技術名	概要	期待される効果	備考
DEP	（省略）	（省略）	プログラムによっては適用できない。
SSP（Stack Smashing Protection）	スタック領域で canary と呼ばれる値を利用してスタックバッファオーバフローの有無を確認する技術	スタックバッファオーバフローを検知し，抑制する。	（省略）
ASLR（Address Space Layout Randomization）	プログラムの実行時に，データ領域，ヒープ領域，スタック領域及びライブラリを，ランダムにマップする OS の技術	（省略）	32 ビット OS の場合，効果が限定的である。
PIE（Position Independent Executable）	プログラムの実行時に，ASLR が対象とする領域に加えて，テキスト領域もランダムにマップする技術	（省略）	プログラムによっては適用できない。
Automatic Fortification	バッファオーバフロー脆弱性の原因となりうる脆弱なライブラリ関数を，コンパイル時に境界チェックを行う安全な関数に置換する技術	境界チェックによって，オーバフローを抑制する。	境界チェックにおいて，書込み先のサイズが不明な場合は機能しない。

〔M 対策技術の動作概要〕

例えば，Vuln のコンパイル時に SSP が適用されていると，関数 foo を呼び出す際，図 2 のベースポインタレジスタ保存値より下位に［　e　］が挿入される。もしも，［　e　］が上書きされた場合は，攻撃と判断し，Vuln の実行を停止する。

なお，Vuln の場合は簡単ではないが，攻撃者が［　e　］の値を正確に推測して上書きできてしまうと，［　a　］の書換えが可能となり，［　d　］攻撃を防げない。その対策としては，ライブラリ関数のアドレス推定を困難にさせる［　f　］が有効である。

しかし，［　f　］は［　c　］領域にある実行可能なコードを用いる攻撃に対しては効果がない。そうした攻撃は PIE によって緩和される。さらに，Vuln の場合，Automatic Fortification によって，ライブラリ関数［　g　］を安全な関数に置き換えることで，バッファオーバフローの原因を排除することができる。

〔脆弱性対策強化〕

L 部長と X 主任が表 1 の技術を確認したところ，表 1 の備考欄の指摘以外にも②

Automatic Fortification ではバッファオーバフローの原因を排除できないケースがあると分かった。

L 部長は次に，表 1 の技術を適用することによる影響を確認した。その結果，次のことが分かった。例えば，ソースコードに脆弱性があっても，SSP を適用してコンパイルしていると，メモリ破壊攻撃が成立しないが，そのソースコードを③別の開発環境でコンパイルすると問題となる場合があることが分かった。

これらについては，U 社内でコーディングスタンダードを定め，それによって対処することにした。検討の結果，U 社は表 1 の技術を全て採用することにした。

設問 1　〔メモリ破壊攻撃の概要〕について，(1) ～(3) に答えよ。

(1) 本文中の［ a ］～［ d ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　Return-to-libc　　イ　ROP

ウ　テキスト　　エ　ヒープ

オ　ベースポインタレジスタ保存値　　カ　ライブラリ

キ　リターンアドレス X

(2) 本文中の［ あ ］に入れる適切なアドレス値を図 2 中から選び，㋐ ～ ㋔ の記号で答えよ。

(3) 本文中の下線①について，攻撃が成功しない理由を 35 字以内で述べよ。

設問 2　〔M 対策技術の動作概要〕について，(1)，(2) に答えよ。

(1) 本文中の［ e ］，［ f ］に入れる適切な字句を，表 1 中の用語を用いて答えよ。

(2) 本文中の［ g ］に入れる適切なライブラリ関数名を答えよ。

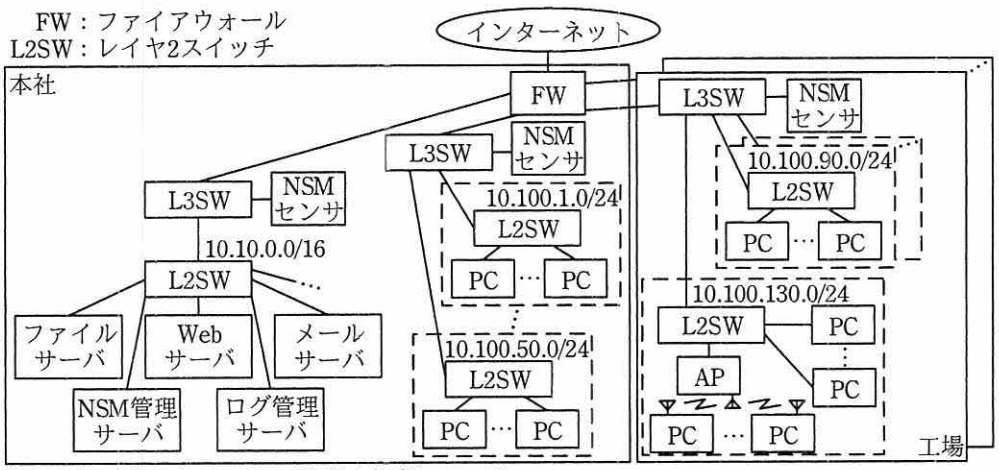
設問 3　〔脆弱性対策強化〕について，(1)，(2) に答えよ。

(1) 本文中の下線②について，図 1 のプログラムにおいて，排除できないケースに該当する処理を行番号で答えよ。また，排除できない理由を 30 字以内で述べよ。

(2) 本文中の下線③について，どのような問題か。また，どのような開発環境の場合に問題となるか。それぞれ 25 字以内で述べよ。

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。

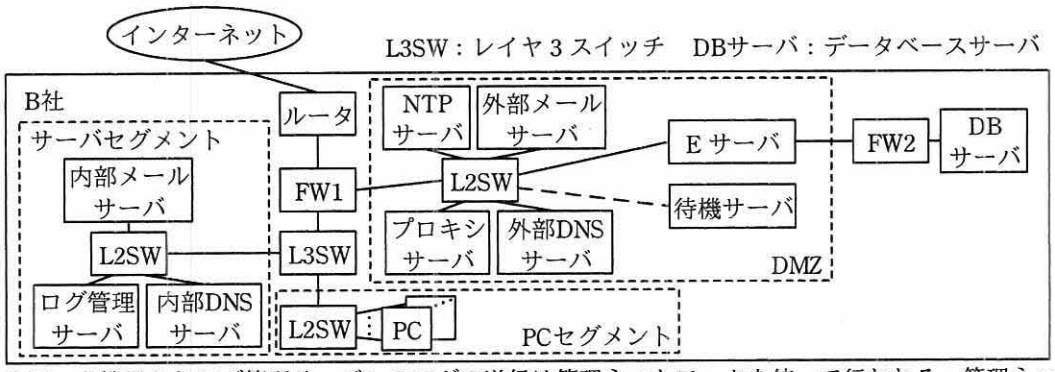
問３　ソフトウェアの脆弱性対策に関する次の記述を読んで，設問 1～5 に答えよ。

B 社は，従業員数 500 名の食品販売会社であり，インターネットを介して消費者向けに食品を通信販売している。

通信販売で使用するシステム（以下，通販システムという）の運用，保守は，B 社の K リーダを中心に，S 君ほか 3 名と協力会社の従業員 5 名の計 10 名で行っている。通販システムを含む B 社情報システムのサーバの概要を表 1 に，構成を図 1 に示す。

表 1　B 社情報システムのサーバの概要（抜粋）

サーバ名	概要
E サーバ	・通販システムの購入受付処理を行う Web サーバである。また，通販システムのバッチ処理として購入集計処理も行っている。
待機サーバ	・E サーバの購入受付処理が停止するなど通販システムの利用者にサービスが提供できなくなった場合に，サービス停止を告知するための Web サーバである。コールドスタンバイしており，E サーバがサービス提供できなくなった場合に E サーバの代わりにレイヤ 2 スイッチ（以下，L2SW という）に接続される。
ログ管理サーバ	・B 社情報システム中の全ファイアウォール（以下，ファイアウォールを FW という）及び全サーバのログを syslog で受信し保存する。 ・FW1 及び FW2 のログには，通信の通過や遮断に関する記録がある。 ・各サーバのログには，OS 上で実行される SSH などのコマンド履歴，アプリケーションやミドルウェアのイベント記録がある。 ・Web サーバ及びプロキシサーバのログには，送信元及び宛先の IP アドレス，HTTP リクエストの内容，データ転送量などが含まれている。 ・ログ保全機能があり，それによって，保存したログが改ざんされていないことを証明できる。



注記　各機器からログ管理サーバへのログの送信は管理ネットワークを使って行われる。管理ネットワークの記載は省略している。

図 1　B 社情報システムの構成

通販システムは，E サーバ，待機サーバ，FW2 及び DB サーバから構成される。E サーバの購入受付処理は，インターネットから HTTP over TLS（以下，HTTPS という）でアクセスされる。購入集計処理は，バッチプログラムで実行される。毎日午前 2 時開始の日次，毎週土曜日の午前 3 時開始の週次，毎月 1 日午前 4 時開始の月次のバッチプログラムがあり，それぞれ 1 時間以内で処理が完了する。

ログ管理サーバに保存されたログからイベントの発生順序を正しく追跡できるように，①ログに書かれる各 FW 及び各サーバの時刻を整合させている。

FW1 はステートフルパケットインスペクション型で，インターネットと通販システム間の通信は，インターネットから E サーバ及び待機サーバへの HTTPS アクセスとその応答が許可されている。そのほかのインターネットと DMZ 内のサーバ間の通信は，各サーバのサービスに必要なものだけ許可している。

プロキシサーバが中継するのは PC セグメントからインターネットへの通信だけである。

〔脆弱性情報の公開と対応〕

ある日，S 君は，アプリケーションフレームワーク（以下，AF という）のうち，E サーバで使用しているもの（以下，E-AF という）の脆弱性（以下，脆弱性 T という）の情報が，前日に公開されていることを発見し，K リーダに報告した。脆弱性 T の情報を図 2 に示す。

・悪用されるとリモートから任意の OS コマンドを実行されるおそれがある。具体的には，リモートから HTTP リクエストの Content-Type ヘッダフィールドに攻撃コードが挿入されることによって任意の OS コマンドを実行される。
・既に攻撃コードやリモート操作用のツールが流通しており，［ a ］[1]による深刻度が高い。

注[1] ［ a ］は，基本評価基準，現状評価基準，環境評価基準の三つの基準で脆弱性の深刻さを評価するシステムである。

図 2　脆弱性 T の情報（概要）

脆弱性 T の情報が公開されると同時に，E-AF の脆弱性修正プログラム（以下，パッチという）が公開されていたが，K リーダは，パッチを適用するには，通販システムの動作に影響がないことの確認が必要な上，もし何らかの影響がある場合，通販

システムを修正するなど時間が掛かることになり，営業上大きな機会損失となることを懸念した。K リーダは，パッチを適用するために通販システムを直ちに停止させるよりも，当面は稼働を継続させつつ，半月後の定期メンテナンス作業時に，影響の確認と必要な修正をできるだけ短時間に実施する方が望ましいと考えた。

〔セキュリティインシデントの発生と対処〕

脆弱性 T の情報を S 君が発見してから 2 日後，E サーバの日次バッチ処理が異常終了するという事象が発生した。S 君が確認したところ，日次バッチプログラムの内容が，見覚えのないスクリプト（以下，スクリプト U という）に書き換えられていた。スクリプト U は，B 社と関係のないサイト Z からプログラムをダウンロードして起動したり，コマンド履歴を参照したりするなどの内容であった。

S 君は，スクリプト U を外部記憶媒体に証拠保全した後，日次バッチプログラムをリカバリした。リカバリ後，日次バッチプログラムを実行し，正常に処理されたことを確認した。さらに，E サーバのほかのバッチプログラムを調査して，改ざんされていないことを確認し，K リーダに状況を報告した。

K リーダは，顧客データが大量に漏えいするなどの重大なセキュリティインシデント（以下，セキュリティインシデントをインシデントという）の可能性もあると考え，専門家による調査を緊急に行うことを経営陣に提案した。K リーダは経営陣の承認を得て，②被害拡大を防止するために必要な措置を S 君に指示するとともに，セキュリティ専門会社にインシデントの調査を依頼した。

〔インシデントの調査〕

依頼を受けたセキュリティ専門会社は，インシデントを調査し，3 日後に調査結果を B 社に報告した。セキュリティ専門会社による調査結果を図 3 に示す。

調査によって，次が判明した。
(1) 脆弱性 T を悪用した攻撃の痕跡が見つかった。
(2) スクリプト U は，次の二つを並列で実行するものであったことから，今回の攻撃の主たる目的は，仮想通貨採掘用プログラム（以下，AP1 という）を実行することであったと考えられる。
  a) AP1，及び AP1 を動作させるのに必要な複数のライブラリをサイト Z から HTTP を使ってダウンロードし，AP1 を実行する。
  b) コマンド履歴から，SSH コマンドの接続先 IP アドレスを全て抽出する。IP アドレスが抽出された場合は，IP アドレスで示される各機器に対し，SSH コマンドで接続を試行し，成功するとその機器上でスクリプト U を実行する。IP アドレスが抽出されなかった場合は，何もしない。
(3) FW1 のログを調査した結果，上記(2)a)でのダウンロードは，FW1 でブロックされていた。また，B 社情報システムのどの機器にも AP1 は見つからなかった。
(4) ③E サーバのコマンド履歴には，SSH コマンドの接続先 IP アドレスが含まれておらず，スクリプト U によるほかの機器への接続はなかったと考えられる。このことを確認するために，ほかの機器へのアクセス記録を調査したところ不審なものはなかった。
(5) 顧客データが大量に漏えいした可能性は低い。

図 3　セキュリティ専門会社による調査結果（抜粋）

重大な被害は認められなかったものの，脆弱性 T が悪用されて改ざんが行われていたことが明らかになったことから，パッチを適用することにした。パッチを適用し，サービスを再稼働できたのは，インシデント発生から 10 日後だった。

〔リスク軽減策の検討〕

セキュリティ専門会社からは，脆弱性情報が公開されると，その後間もなく攻撃が急増することが多いことから，脆弱性情報が公開された際に迅速に対応できるようにあらかじめ対応を検討しておくべきであるとアドバイスを受けた。そこで，今回のインシデントも踏まえて，K リーダと S 君は AF などを利用しているシステムの脆弱性が公開された際の対応について検討した。次は，このときの S 君と K リーダの会話である。

S 君　　：AF の脆弱性情報が公開された際は，早期に対応することが望まれます。その点では，暫定的な対策として WAF の導入が有効との話をよく聞くので，調査しました。
K リーダ：どうだったかな。
S 君　　：脆弱性 T については，情報が公開されてから 1 日以内にシグネチャが提供された WAF がありました。

Kリーダ　：通販システムではパッチの適用作業に 7 日掛かったが，それより，WAF による対応の方が早かったようだな。しかし，WAF による対応では，通販システムへの影響があるのではないか。

S君　　：影響があるので，導入時には遮断はせずにアラートを通知するだけのモニタリングモードを用いて検証します。ただし，このモードでは，アラートが通知された際に検知した通信が［　b　］であるかどうかを直ちに確認しなければなりません。もし，［　b　］であった場合は，場合によっては E サーバの停止が必要となります。また，［　b　］ではなかった場合は，WAF のシグネチャの見直しが必要となります。これら一連の手順を決めておかなければなりません。

Kリーダ　：分かった。次に，WAF の選定方法について，確認しておこう。

S君　　：WAF には，大きく分けると，ソフトウェア型，ハードウェア型，クラウド型の 3 種類があります。いずれもモニタリングモードを実現する機能と攻撃とみなされる通信を遮断する機能があります。さらに，④暗号通信に関する機能が用意されているものがあります。

Kリーダ　：なるほど。導入はどのようにするのかな。

S君　　：ソフトウェア型 WAF の場合は，E サーバに導入します。ハードウェア型 WAF の場合は，図 1 中の DMZ 内の L2SW と E サーバとの間に設置します。クラウド型 WAF の場合は，サービス事業者がインターネット上で運用しているものを利用します。クラウド型 WAF を利用する場合は，幾つか設定変更が必要です。例えば，図 1 中の［　c　］の設定を変更して，E サーバへのアクセス経路をクラウド型 WAF 経由に変える必要があります。クラウド型 WAF の IP アドレスが変更された場合でも［　c　］の設定に影響が出ないように，［　d　］レコードを定義して，そのレコードに E サーバの別名としてクラウド型 WAF サービスの事業者が指定する FQDN を記述することが推奨されています。

Kリーダ　：なるほど。当社にはどの種類が適しているか調査してくれ。

S君　　：分かりました。

調査の後，B 社では，WAF を選定し，導入した。以降，攻撃を数多く受けたが，WAF が遮断し，E サーバへの侵入は起きていない。

設問1　本文中の下線①を実現するための手段を 15 字以内で述べよ。

設問2　図 2 中の［　a　］に入れる適切な字句を英字 4 字で答えよ。

設問3　本文中の下線②について，K リーダが S 君に指示した措置を，30 字以内で述べよ。

設問4　図 3 中の下線③について，コマンド履歴に SSH コマンドの接続先 IP アドレスが含まれていた場合，スクリプト U の内容を考慮すると更に調査が必要となる。仮に接続先 IP アドレスとして外部メールサーバが履歴に含まれていた場合，どの機器のログで，何を調査すべきか。調査すべき機器の名称を図 1 中から選び答えよ。また，調査すべき内容を 30 字以内で，具体的に述べよ。

設問5　〔リスク軽減策の検討〕について，(1)～(3)に答えよ。

(1)　本文中の［　b　］に入れる適切な字句を 5 字以内で答えよ。

(2)　B 社で，ハードウェア型 WAF を導入する場合，通販システム利用者の通信プロトコルを考慮すると本文中の下線④の機能が必要である。その機能を 30 字以内で具体的に述べよ。

(3)　本文中の［　c　］に入れる適切なサーバ名を図 1 中から選び答えよ。また，本文中の［　d　］に入れる適切なレコードの名称を答えよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。