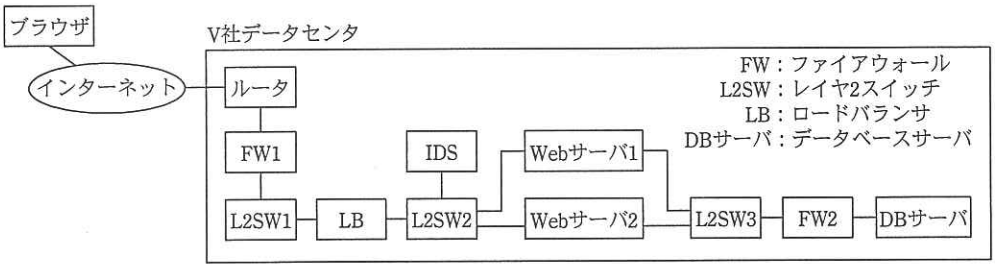
問4　情報セキュリティインシデント対応に関する次の記述を読んで，設問1～3に答えよ。

W社は，地方都市を拠点とする人材派遣会社で，従業員数は60名である。W社では，インターネット上のWebサイト（以下，人材情報サイトという）で，派遣社員登録希望者に対して，W社への登録，求人情報の閲覧などができるサービスを，3年前から提供している。

派遣社員登録希望者は，まず，人材情報サイトから個人プロフィールをW社に送信する。次に，面接を受けて合格すれば，W社に正式登録され，非公開求人情報の閲覧，W社の担当者への相談が可能になる。

〔人材情報サイトの概要〕

人材情報サイトは，V社のデータセンタに設置されている。人材情報サイトのネットワーク構成を図1に，人材情報サイトの機器のFQDN及びIPアドレスを表1に，人材情報サイトの概略を図2に示す。



注記　図中の管理用セグメントは省略

図1　人材情報サイトのネットワーク構成

表1　人材情報サイトの機器のFQDN及びIPアドレス（抜粋）

機器名称	FQDN	IPアドレス	説明
FW1	－	□□.2.2.1	FW1のインターネット側IPアドレス
	www.w-sha.co.jp	□□.2.2.2	Webサーバの仮想IPアドレス
	－	192.168.0.1	FW1のLB側IPアドレス
LB	－	192.168.0.3	LBのインターネット側IPアドレス
	－	192.168.0.10	Webサーバの仮想IPアドレス
	－	192.168.1.254	LBのWebサーバ側IPアドレス
Webサーバ1	－	192.168.1.11	Webサーバ1のインターネット側IPアドレス
Webサーバ2	－	192.168.1.12	Webサーバ2のインターネット側IPアドレス

注記　表中の□□は，特定の数字を表す。

(1) 利用者は，ブラウザからインターネットを経由して人材情報サイトを利用する。ブラウザからのアクセスは，LB によって 2 台の Web サーバ（2 台を合わせて Web サーバ群という）に負荷分散される。

(2) Web サーバ上では，次の四つが稼働している。

・OS

・HTTP による送受信を処理する Web サーバプログラム

・Web アプリケーションを動作させるためのミドルウェア

・Web アプリケーション

Web アプリケーションは，ミドルウェア経由で DB サーバにアクセスする。ブラウザからのアクセスについて，Web サーバプログラムが処理する最大同時セッション数は，Web サーバプログラムで 50 に制限している。LB では，任意の HTTP ヘッダフィールドを追加可能であるが，現在は何も追加していない。追加した HTTP ヘッダフィールドは，全て Web サーバのアクセスログに出力可能である。

(3) Web アプリケーションの開発は，W 社の情報システム部で行っている。

(4) 機器のハードウェア保守は，V 社に業務委託している。OS を含むソフトウェアのバージョン管理及びバージョンアップは，W 社の情報システム部で行っている。全ての機器の時刻は，V 社の NTP サーバを利用して同期させている。

(5) FW は，パケットフィルタリング型である。

(6) IDS は，L2SW2 のミラーポートを監視対象とし，トラフィックに対してシグネチャとのパターンマッチングを行い，攻撃を検知する。アラートレベルは，High，Medium 及び Low に分けられており，High の場合だけアラートが IDS から管理用セグメントを経由して W 社情報システム部の運用チーム（以下，運用チームという）に電子メールで通知される。シグネチャは，製品の標準設定で自動更新されるようになっている。

(7) LB は，SSL アクセラレータ機能と負荷分散機能を提供しており，Web サーバの仮想 IP アドレスをもち，2 台の Web サーバにアクセスを負荷分散する。また，Web サーバ群の死活監視機能をもち，負荷分散対象である Web サーバの TCP8443 番ポートに，1 分間に一度アクセスしてサービスの稼働チェックを行う。アクセスしてから 30 秒以内に死活監視用コンテンツを取得できない場合は，サービスダウンとみなして警告（以下，サービスダウンとみなした警告をイベント通知という）を発し，運用チームに電子メールで通知する。サービスダウンの Web サーバにはリクエストを送らない。また，HTTP ヘッダフィールドとして X-Forwarded-For ヘッダフィールドを追加可能であるが，現在は利用していない。

図 2　人材情報サイトの概略

〔インシデントの発生〕

ある月曜日の朝，LB のイベント通知が発生した。運用チームの G 主任が，原因を調査することになった。G 主任が，運用チームの Web サーバ管理担当者 H さんに確認したところ，Web サーバプログラムで制限している最大同時セッション数が不足してイベント通知が発生したとの報告を受けた。人材情報サイトは，リリース後にアクセス数が増加しているので，最大同時セッション数の設定の見直しを運用チーム内で検討していた。特に月曜日は，求人情報の定期更新があり，16 時まではアクセスが集中する。そこで，たとえイベント通知が発生しても，次のサービス稼働チェックで復旧した場合は無視することにした。ところが，16 時を過ぎてもイベント通知が発生した

ので，G 主任は改めてイベント通知の原因の調査を開始した。

G 主任は，①各機器の当日のログを調査した結果，人材情報サイトが攻撃を受けていた可能性が高いと判断した。LB のサービス稼働チェックログを表 2 に，IDS がシグネチャ A に該当するとして検知した事象のログを表 3 に，表 3 の各事象に関する FW1 のログを表 4 に，同じく表 3 の各事象に関する Web サーバ 1，2 のアクセスログを表 5，表 6 に，Web サーバ群のリソースグラフを図 3 に示す。

なお，各ログは，調査で確認した当日の各機器の大量のログから抜粋したものである。

表 2　LB のサービス稼働チェックログ（抜粋）

検知時刻	監視対象 IP アドレス	ステータス
10:05:00	192.168.1.11	down
10:06:00	192.168.1.11	up
11:01:00	192.168.1.11	down
11:02:00	192.168.1.11	up
12:15:00	192.168.1.12	down
12:16:00	192.168.1.12	up
13:02:00	192.168.1.12	down
13:03:00	192.168.1.12	up

検知時刻	監視対象 IP アドレス	ステータス
14:00:00	192.168.1.12	down
14:01:00	192.168.1.12	up
15:05:00	192.168.1.11	down
15:06:00	192.168.1.11	up
18:51:00	192.168.1.12	down
18:52:00	192.168.1.12	up
19:23:00	192.168.1.11	down
19:24:00	192.168.1.11	up

注記 1　ステータスが down のもの及びその 1 分後のものの抜粋
注記 2　表中の検知時刻は，稼働チェック用のリクエストを送信した時刻を表す。

表 3　IDS の検知ログ（シグネチャ A 検知に関連するログの抜粋）

項番	検知時刻	アラートレベル	送信元 IP アドレス	宛先 IP アドレス	送信元 ポート番号	宛先 ポート番号
(1)	11:00:12	Low	192.168.1.254	192.168.1.11	19212	8443
(2)	13:21:06	Low	192.168.1.254	192.168.1.12	14506	8443
(3)	15:04:54	Low	192.168.1.254	192.168.1.11	39871	8443
(4)	16:59:23	Low	192.168.1.254	192.168.1.11	40192	8443
(5)	18:50:20	Low	192.168.1.254	192.168.1.12	10211	8443
(6)	19:22:43	Low	192.168.1.254	192.168.1.11	50983	8443

表４　FW1 のログ（シグネチャ A 検知に関連するログの抜粋）

項番	処理時刻	処理	プロトコル	送信元 IP アドレス	宛先ポート番号	送信バイト数
(1)	11:00:12	許可	TCP	△△.123.123.123	443	6,401,200
(2)	13:21:06	許可	TCP	○○.1.1.1	443	301,201
(3)	15:04:54	許可	TCP	△△.123.123.123	443	6,401,121
(4)	16:59:23	許可	TCP	○○.1.1.2	443	305,121
(5)	18:50:20	許可	TCP	△△.123.123.123	443	6,401,220
(6)	19:22:43	許可	TCP	△△.123.123.123	443	6,401,198

注記　表中の△△，○○は，特定の数字を表す。

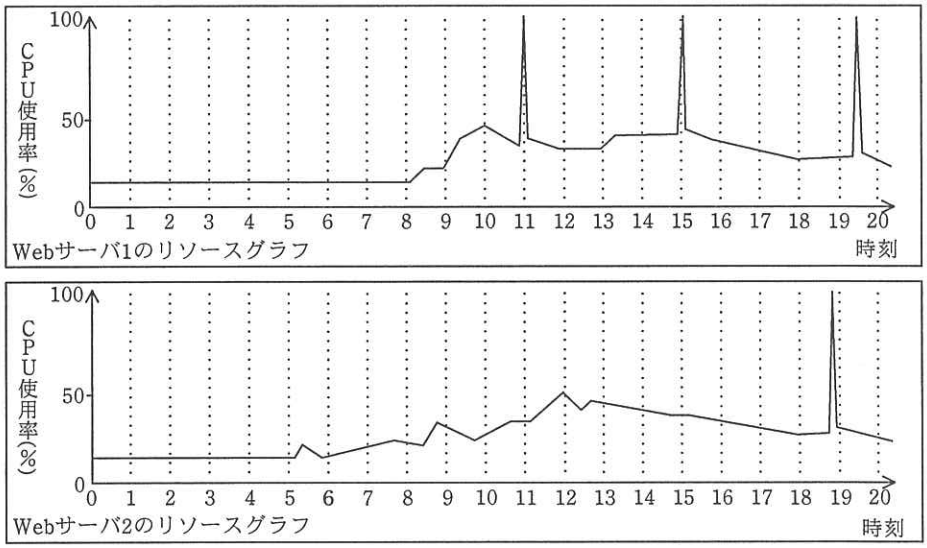


図３　Web サーバ群のリソースグラフ

表５　Web サーバ１のアクセスログ（シグネチャ A 検知に関連するログの抜粋）

項番	送信元 IP アドレス	アクセス 時刻	リクエスト内容	ステータス コード	受信バイト数
(1)	192.168.1.254	11:00:12	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,124
(2)	192.168.1.254	15:04:54	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,011
(3)	192.168.1.254	16:59:23	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	200	305,071
(4)	192.168.1.254	19:22:43	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,162

表6　Webサーバ2のアクセスログ（シグネチャA検知に関連するログの抜粋）

項番	送信元IPアドレス	アクセス時刻	リクエスト内容	ステータスコード	受信バイト数
(1)	192.168.1.254	13:21:06	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	200	301,143
(2)	192.168.1.254	18:50:20	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,181

〔暫定対策の実施〕

IDSが通知したアラートと，その際にIDSが内部に保存したパケットデータをIDS販売元のセキュリティベンダX社に提供して問い合わせた結果，数日前に情報が公開されたばかりの脆弱性を狙った攻撃であることが判明した。その脆弱性は，特定のデータを受信するとWebサーバのCPUリソースが一時的に枯渇するというものであった。X社からは，ミドルウェアをバージョンアップすることによって，脆弱性を除去できるという回答があった。しかし，Hさんが帰宅してしまっていたので，すぐにはバージョンアップができなかった。そこで，攻撃元だと特定したIPアドレス［　a　］からの通信をFW1で遮断することにした。

また，IDSでは，シグネチャAの検知基準が，標準設定の“HTTP POSTリクエストが300,000バイト以上”だった。したがって，②誤検知が発生する可能性が高く，それを考慮して，アラートレベルはLowにしていた。しかし，アラートレベルがLowではメール通知がされないので，Highに変更すべきかX社に相談したところ，もしアラートレベルをHighにするのであれば，誤検知を減らすために検知基準を変更した方がよいという助言を受けた。そこで，今回の脆弱性を狙った攻撃を検知可能で，かつ，誤検知が減るように検知基準を変更した上で，アラートレベルをHighに変更した。

〔恒久対策の検討と運用強化〕

その後W社では，シグネチャAのアラートは通知されなかった。Hさんはミドルウェアのバージョンアップの影響を調査した後，バージョンアップを実施し，今回の脆弱性への対策を完了した。さらに，セキュリティ運用について情報システム部内で課題を洗い出し，次のような対策案を作成した。

(A) 脆弱性情報の把握と対策の早期実施

IPA及びJPCERT/CCから公開される脆弱性情報を確認し，人材情報サイトに影響を及ぼす脆弱性があれば，速やかに対策を講じる。また，その脆弱性を狙った攻撃

を IDS が検知できる場合は，その脆弱性を検知するシグネチャのアラートレベルを，人材情報サイトへの影響度に見合ったレベルに設定する。

(B) Web サーバのサービス稼働チェックの最適化

Web サーバのサービス稼働チェックでは，対処する必要がない場合でもイベント通知している。対処が必要な場合にだけイベント通知するように，③Web サーバの設定を変更の上，イベント通知すべき条件を変更する。

(C) 相関分析を目的としたログ調査環境・手順の整備

今回は同時に大量のアクセスが発生したので，大量のログから攻撃元を特定するまでに時間が掛かった。今後は，④攻撃元を特定しやすくするために，FW1 と Web サーバ群のログを関連付けられるようにログの出力内容と分析手順を見直す。また，IDS については，L2SW2 のトラフィックの代わりに L2SW1 のトラフィックを監視対象にすることによって，ネットワークアドレス変換前の [b] を確認できるので，攻撃元の特定が容易になる。ただし，LB への [c] 通信については監視できないので，IDS は LB が保有している [d] を利用して [c] 通信についても監視できるものにする。

これらの対策案を基に，W 社ではセキュリティ運用を強化することにした。

設問 1 本文中の下線①について，G 主任は，表 2 によって事象の発生時間帯をある程度絞り込んだ後，更に絞り込むため図 3 に着目した。G 主任が，図 3 に着目した理由は何か。50 字以内で述べよ。

設問 2 〔暫定対策の実施〕について，(1)～(3)に答えよ。

(1) 本文中の [a] に入れる IP アドレスを，表 4 の中から選んで答えよ。

(2) 本文中の下線②について，表 3 の IDS の検知ログには幾つかの誤検知が含まれている。それらが誤検知であるということは，表 5，表 6 のどのアクセスログから判断できるか。表 5，表 6 から全て選び，例えば，表 5 の項番(1)の場合は，“表 5(1)”のように，表番号と項番の組合せで答えよ。

(3) 上記(2)で誤検知であると判断した理由を，35 字以内で述べよ。

設問 3　〔恒久対策の検討と運用強化〕について，(1)～(3)に答えよ。

(1) 本文中の [b] ～ [d] に入れる適切な字句を，[b] は 10 字以内，[c]，[d] はそれぞれ 5 字以内で答えよ。

(2) 本文中の下線③について，Web サーバの設定変更を実施することによって改善される，不要なイベント通知の原因になっていた Web サーバ内の事象を，35 字以内で述べよ。

(3) 本文中の下線④について，FW1 と Web サーバ群のログを関連付けられるようにするために設定変更が必要な機器はどれか。解答群の中から二つ選び，記号で答えよ。また，それぞれの設定内容を 40 字以内で述べよ。

解答群

ア　ルータ　　イ　FW1　　ウ　LB　　エ　IDS

オ　Web サーバ群