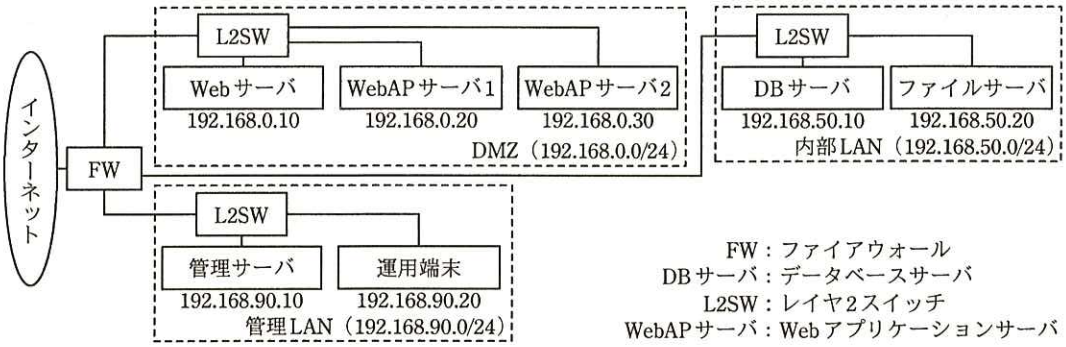
問3　Web サイトにおけるインシデント対応に関する次の記述を読んで，設問 1～4 に答えよ。

W 社は，精密機器を製造している従業員数 500 名の会社である。W 社では，取引先との間で設計データを共有するために Web サイト（以下，サイト X という）を利用している。サイト X は，W 社の情報システム部が開発，運用しており，W 社の従業員と取引先の従業員が利用している。サイト X のネットワーク構成を図 1 に，システム概要を図 2 に示す。



注記 1　192.168.0.0/24，192.168.50.0/24，192.168.90.0/24 は，ネットワークアドレスを示す。
注記 2　DMZ の各サーバに対しては FW で NAT の設定がされている。

図 1　サイト X のネットワーク構成

・Web サーバでは，インターネットに静的コンテンツを公開している。
・負荷分散のために，WebAP サーバ 1 及び WebAP サーバ 2 の 2 台構成になっており，Java で開発した Web アプリケーションソフトウェア（以下，Web アプリケーションという）がサーブレットコンテナで稼働している。Web アプリケーションは，JDBC[1]接続を使って DB サーバに，OS のファイル共有機能を使ってファイルサーバにそれぞれアクセスする。
・WebAP サーバ 1 及び WebAP サーバ 2 のサーブレットコンテナの管理画面には，管理画面用の利用者 ID でログインできる。管理画面へのログインは，ベーシック認証で行われる。成功時は 200，失敗時は 401 のステータスコードを返す。管理画面では，Web アプリケーションのアップロードと配置ができる。
・DB サーバでは，DBMS の監査ログを取得するよう設定している。
・管理サーバでは，各サーバに導入したエージェントソフトを使ってログを集中管理している。
・運用端末では，ファイル共有とリモートデスクトップのサービスを使用して各サーバを操作できる。
・各サーバ及び運用端末では，OS として Windows を使っている。各サーバ及び運用端末には，利用者 ID として，“administrator” と “unyou” の二つを用意している。いずれも管理者権限の利用者 ID である。
・サーブレットコンテナのプロセスは，“administrator” の権限で動作しており，管理画面と Web アプリケーションも，“administrator” の権限で動作する。
・各サーバ及び運用端末では，Web サーバ上で稼働している NTP サーバとの間で，NTP を用いて時刻同期をしている。

注 1)　JDBC は，Java からデータベースに接続するための API である。

図 2　サイト X のシステム概要

〔セキュリティインシデントの発生〕

ある日，DMZ に設置している 3 台のサーバで，同様のタスク実行失敗を示すイベントが出力されたので，サイト X の運用を担当している B 氏は，システム障害として調査を行った。DMZ の各サーバのイベントログを表 1 に示す。

表 1　DMZ の各サーバのイベントログ

日時	ログメッセージ
2015/01/22 12:52:00	タスクスケジューラは，利用者 ID “administrator” の “printer” タスクを開始できませんでした。

調査の結果，図 3 の事象が確認できたことから，B 氏は，不正侵入のセキュリティインシデントが発生したと判断した。

・OS のタスクスケジューラに，業務上必要のないタスクが登録されており，そのタスクは実行が失敗していた。
・“C:¥Temp¥printer” の場所に，“info.bat” と “info.txt” というファイルが作成されていた。“info.bat” は，バッチファイルであり，システム構成情報と利用者情報を取得するコマンドを実行して，結果を “info.txt” という名前のファイルに出力する。

図 3　DMZ の各サーバで発生した事象

B 氏は，DMZ のサーバ 3 台をネットワークから切り離し，取引先にサイト X の停止を通知した後，セキュリティ担当 A 氏の協力を得て，侵入経路の調査を開始した。

〔侵入経路の調査〕

A 氏は，DMZ に設置しているサーバの OS へのログイン履歴を基に，タスク実行失敗を示すイベントが出力された日時の前後のログを調査して，どのサーバが最初に侵入されたかを特定した。Web サーバ，WebAP サーバ 1 及び WebAP サーバ 2 の 3 台の 2015 年 1 月 1 日以降のログイン履歴は，表 2～4 のとおりである。

表 2　Web サーバのログイン履歴

日時	接続元 IP アドレス	利用者 ID	ログインの成功失敗
2015/01/07 19:30:16	192.168.90.20	unyou	成功
2015/01/07 19:38:14	192.168.90.20	unyou	成功
2015/01/22 12:03:00	192.168.90.20	unyou	成功
2015/01/22 12:23:00	192.168.90.20	unyou	成功
2015/01/22 12:42:07	192.168.0.20	administrator	成功
2015/01/22 18:11:25	192.168.90.20	unyou	成功

表 3　WebAP サーバ 1 のログイン履歴

日時	接続元 IP アドレス	利用者 ID	ログインの成功失敗
2015/01/05 19:28:46	192.168.90.20	unyou	成功
2015/01/08 20:23:00	192.168.90.20	unyou	成功
2015/01/22 12:32:20	192.168.0.30	administrator	成功

表 4　WebAP サーバ 2 のログイン履歴

日時	接続元 IP アドレス	利用者 ID	ログインの成功失敗
2015/01/06 19:28:21	192.168.90.20	unyou	成功
2015/01/06 19:30:16	192.168.90.20	unyou	成功
2015/01/23 12:03:00	192.168.90.20	unyou	成功

次は，侵入経路の調査の過程における A 氏と B 氏の会話である。

A 氏：ログイン履歴には，複数の利用者 ID のログインが記録されています。利用者 ID はどのように使い分けているのですか。

B 氏：運用では，“unyou”を使用しており，“administrator”は使用していません。

A 氏：そうだとすると，“administrator”という利用者 ID を使ってサーバにログインした者が攻撃者であると推測できます。［ a ］から［ b ］に，［ b ］から［ c ］にという順番でログインしていますね。

B 氏：それでは，最初に侵入されたサーバは，［ a ］ということでしょうか。

A 氏：その可能性が高いですね。侵入された原因を特定するためには，［ a ］のアクセスログを調査する必要があります。

B 氏：ところで，ログイン履歴を見ると，失敗することなく短時間で他のサーバへのログインが成功しています。攻撃者は，どのような方法で他のサーバにロ

グインしたのでしょうか。

A 氏：DMZ の各サーバには，“unyou”，“administrator” という利用者 ID が，全サーバに同じパスワードで設定されているようです。そうした設定では，あるサーバから他のサーバにアクセスする際，自動的にログインが行われます。攻撃者は，そのような OS の仕様を利用して，他のサーバにもログインしたようです。

〔侵入された原因の特定〕

A 氏は，インターネットから侵入された原因を特定するために，［ a ］のアクセスログを調査した。担当者にヒアリングしたところ，設定に誤りがあり，インターネットから管理画面にアクセスできるようになっていたことが分かった。［ a ］のアクセスログのうち，攻撃者の IP アドレスからのものを表 5 に示す。調査の結果，①サーブレットコンテナの管理画面に対して，よく使われる利用者 ID とパスワードでログインが試行され，その結果，ログインが成功したものと推測された。管理画面から，バッチファイルを［ a ］にアップロードされた後，タスクが登録されたり，バッチファイルが実行されたりしたと推測された。

表5 [a] のアクセスログ

No.	時刻	リクエスト	ステータスコード	応答のバイト数
1	10:36:04	GET /test/ HTTP/1.1	404	1,277
2	10:36:23	GET /demo/ HTTP/1.1	404	1,277
3	10:59:12	GET /manager/html HTTP/1.1	401	2,550
4	10:59:12	GET /manager/html HTTP/1.1	401	2,550
5	10:59:12	GET /manager/html HTTP/1.1	401	2,550
6	10:59:12	GET /manager/html HTTP/1.1	401	2,550
7	10:59:13	GET /manager/html HTTP/1.1	401	2,550
8	10:59:13	GET /manager/html HTTP/1.1	401	2,550
9	10:59:13	GET /manager/html HTTP/1.1	401	2,550
10	10:59:13	GET /manager/html HTTP/1.1	401	2,550
11	10:59:14	GET /manager/html HTTP/1.1	200	19,689
12	11:02:09	GET /manager/html HTTP/1.1	200	19,689
13	11:02:27	POST /manager/html/upload HTTP/1.1	200	21,453
14	11:02:34	GET /demo/index.jsp HTTP/1.1	200	2,588
15	11:39:23	GET /demo/index.jsp HTTP/1.1	200	2,588
16	11:39:33	GET /demo/index.jsp?sort=1&dir=C%3A%5C HTTP/1.1	200	3,453
17	11:39:47	GET /demo/index.jsp?sort=1&dir=C%3A%5CTemp HTTP/1.1	200	2,129
18	11:39:52	GET /demo/index.jsp?sort=1&dir=C%3A%5CTemp%5Cprinter HTTP/1.1	200	1,347
19	11:41:02	POST /demo/index.jsp HTTP/1.1	200	3,697
20	11:42:05	POST /demo/index.jsp HTTP/1.1	200	3,697
21	11:42:09	POST /demo/index.jsp HTTP/1.1	200	2,506
22	11:42:18	POST /demo/index.jsp HTTP/1.1	200	2,506
23	11:42:39	GET /demo/index.jsp?sort=1&dir=C%3A%5CTemp%5Cprinter HTTP/1.1	200	1,896

注記　日付は，2015年1月22日である。

次は，[a] のアクセスログの調査過程における A 氏と B 氏の会話である。

A 氏：侵入された後，demo ディレクトリに index.jsp という名前のファイルをアップロードされたようです。アクセスログの No. [d] のステータスコードが [e] であり，No. [f] のステータスコードが [g] であるということから，demo ディレクトリは攻撃者が No. [f] の直前で作成したことが分かります。

B 氏：確かに，[a] には，demo ディレクトリは元々ありませんでした。

A 氏：index.jsp を調査したところ，攻撃ツールであることが分かりました。指定した

ファイルをインターネット上のサーバにアップロードする機能，OS のファイル共有機能を使って他のサーバにファイルを転送する機能，OS のファイル共有機能を使って他のサーバ上で OS コマンドを実行する機能，及び DBMS に対して SQL を発行する機能をもっています。

〔影響範囲の特定〕

A 氏は，内部 LAN 及び管理 LAN への影響を特定するために，FW のフィルタリングルールを確認して，侵入されたサーバからどの範囲がアクセス可能だったかを調査することにした。FW のフィルタリングルールを表 6 に示す。W 社のポリシでは，業務上必要なサービスだけを FW で許可することになっているが，②FW のフィルタリングルールにはポリシを満たしていないものがあることが判明した。

表 6　FW のフィルタリングルール

項番	送信元	宛先	サービス	動作
1	インターネット	192.168.0.10	HTTP	許可
2	インターネット	192.168.0.20，192.168.0.30	HTTP，HTTPS	許可
3	192.168.0.20，192.168.0.30	192.168.50.10	JDBC 接続	許可
4	192.168.0.20，192.168.0.30	192.168.50.20	ファイル共有	許可
5	192.168.90.20	192.168.0.0/24，192.168.50.0/24	全て	許可
6	192.168.90.10	192.168.0.0/24，192.168.50.0/24	ログ収集	許可
7	192.168.50.0/24，192.168.90.0/24	192.168.0.10	NTP	許可
8	192.168.0.10	公的機関の NTP サーバ	NTP	許可
9	全て	全て	全て	拒否

注記 1　項番が小さいものから順に，最初に一致したルールが適用される。
注記 2　FW は，ステートフルインスペクション型のものである。
注記 3　全てのルールについて，ログを取得する設定となっている。

次に，A 氏は，タスク実行失敗を示すイベントが発生した日以降の，FW のログを調査し，内部 LAN 及び管理 LAN への影響がないことを確認した。

〔対策とシステム再稼働〕

A 氏と B 氏は，影響範囲が DMZ のサーバ 3 台だけであったことから，それらのサーバの再構築を行った後，次の対策を実施した。

(a)　WebAP サーバ 1 と WebAP サーバ 2 に，図 4 のアクセス制御の設定を行うことで，送信元の IP アドレスが 127.0.0.1 である場合だけ，サーブレットコンテナの管

理画面へのアクセスを許可する。

```
<Location /manager/>
Order deny,allow
Deny from all
Allow from 127.0.0.1
</Location>
```

図4　アクセス制御の設定

(b)　各サーバの利用者 ID “administrator” を無効化し，利用者 ID “unyou” は，サーバごとに異なる利用者 ID に変更し，さらに，パスワードもサーバごとに異なるものに変更する。

W 社では，B 氏が経営幹部に不正アクセスの調査結果を報告し，承認を得てシステムを再稼働させた後，取引先に通知し，インシデント対応を完了した。

設問1　本文中の［ a ］～［ c ］に入れるサーバ名を，図1中の字句を用いて答えよ。

設問2　〔侵入された原因の特定〕について，(1)，(2)に答えよ。

(1)　本文中の［ d ］～［ g ］に入れる適切な数値を答えよ。

(2)　本文中の下線①のように推測された理由を，表5のログに基づいて 60 字以内で述べよ。

設問3　〔影響範囲の特定〕について，(1)，(2)に答えよ。

(1)　内部 LAN への影響を調査するには，FW のどのフィルタリングルールで取得されるログを確認すればよいか。該当するものを全て，表 6 の項番で答えよ。

(2)　本文中の下線②について，ポリシを満たしていないことが判明したルールはどれか。表 6 の項番で答えよ。また，当該ルールがポリシを満たすように設定すべきサービスを二つ答えよ。

設問4　〔対策とシステム再稼働〕について，本文中の(a)，(b)の対策は，今回のインシデントにおける一連の攻撃のうち，どのような攻撃を防ぐために実施するものか。(a)，(b)について，防ぎたい攻撃をそれぞれ 40 字以内で述べよ。